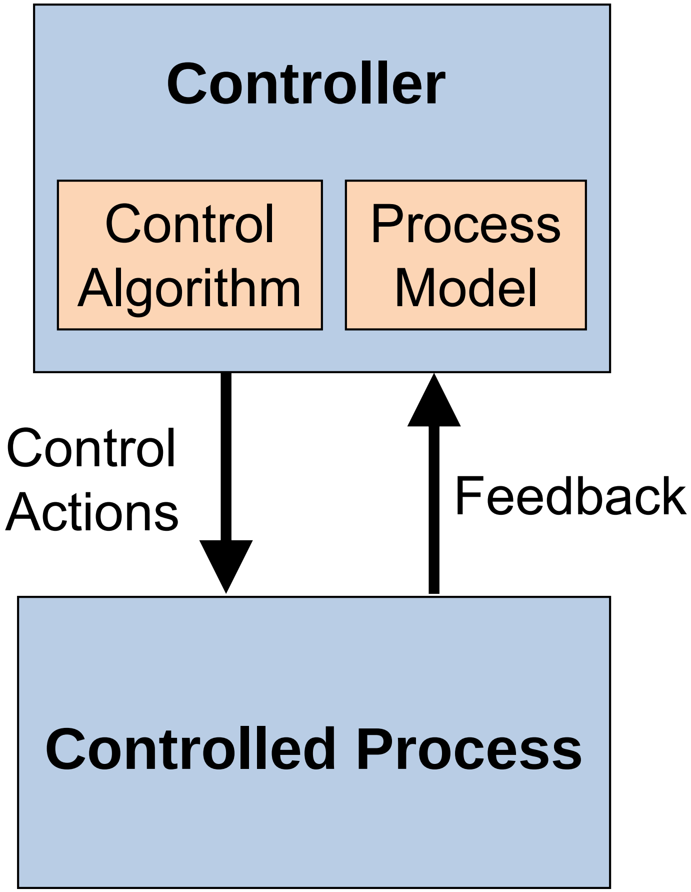
Systems Theoretic Process Analysis (STPA)

Systems approach to safety engineering (STAMP)

STAMP Model

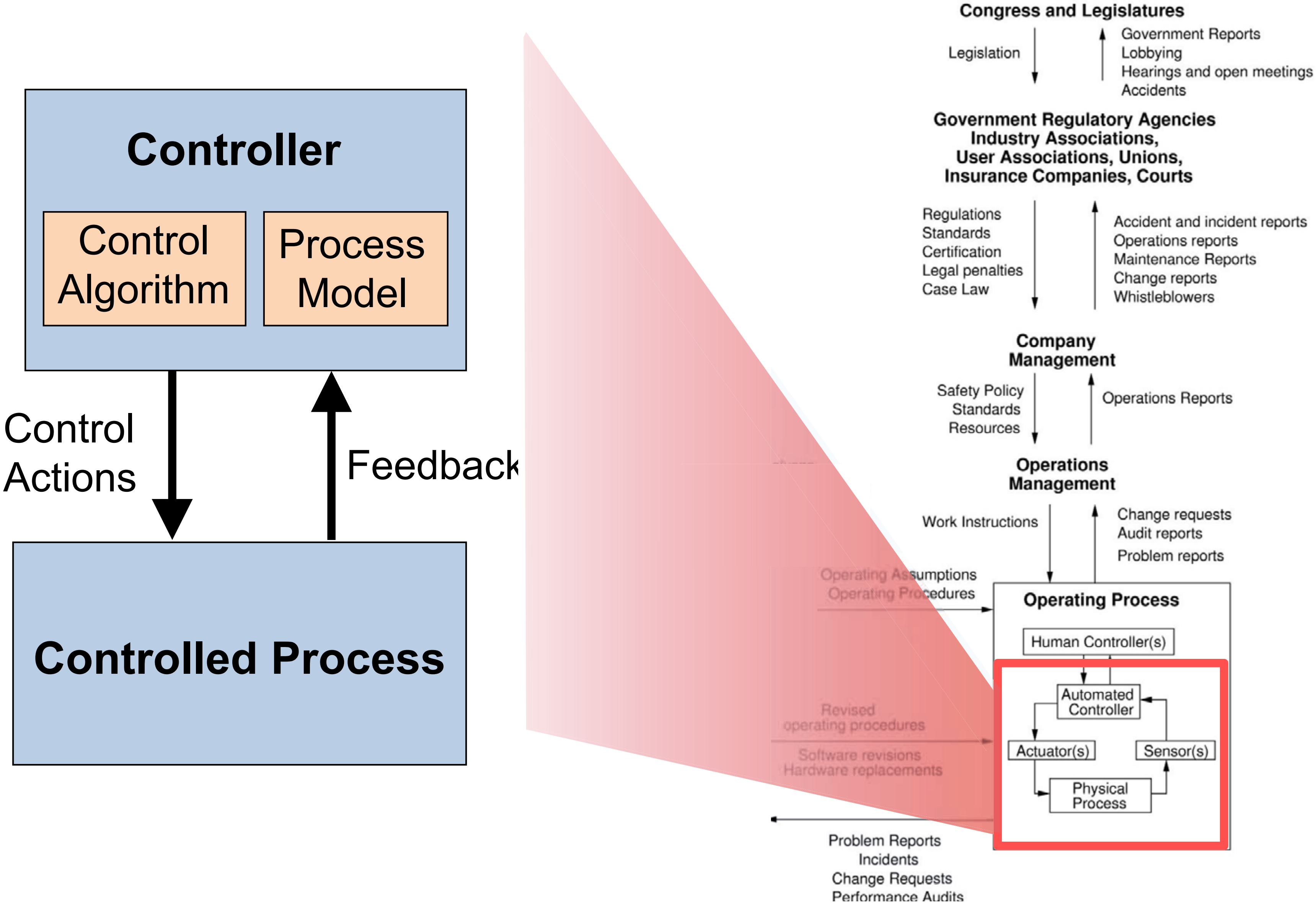
- Accidents are more than a chain of events, they involve complex dynamic **processes**.
- Treat accidents as a **control problem**, not just a failure problem
- Prevent accidents by enforcing constraints on component behavior and **interactions**
- Captures more causes of accidents:
  - – Component failure accidents
  - – Unsafe interactions among components
  - – Complex human, software behavior
  - – Design errors
  - – Flawed requirements
    - esp. software-related accidents

STAMP: basic control loop



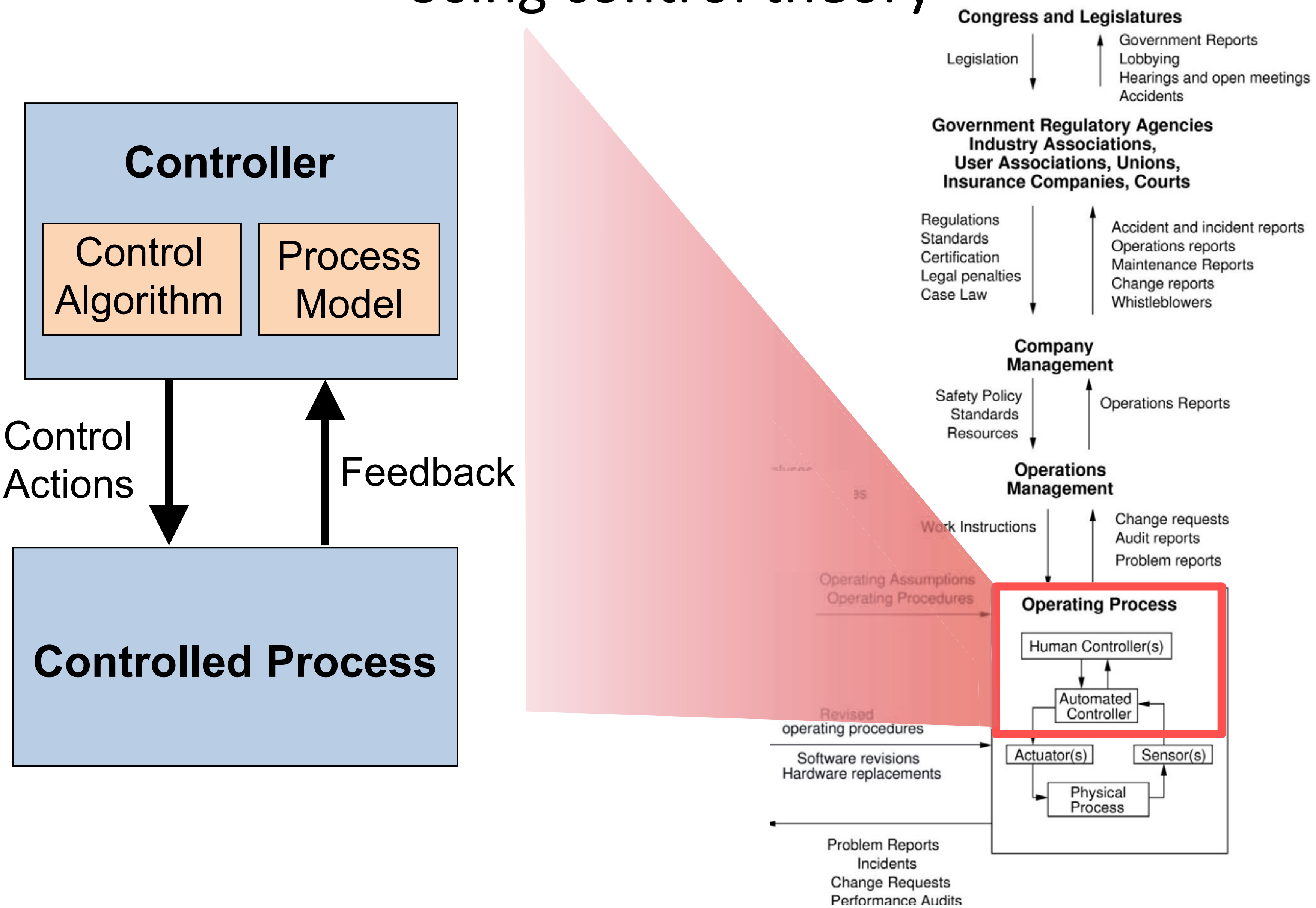
- Controllers use a **<u>process model</u>** to determine control actions
  - Accidents often occur when the process model is incorrect
- A good model of both software and human behavior in accidents
- Four types of **<u>unsafe control actions</u>**:
  1) Control commands required for safety are not given
  2) Unsafe ones are given
  3) Potentially safe commands but given too early, too late
  4) Control action stops too soon or applied too long

Using control theory



From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Using control theory



Controller

Control Algorithm

Process Model

Control Actions

Feedback

Controlled Process

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company
Management

Safety Policy
Standards
Resources

Operations Reports

Operations
Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated
Controller

Actuator(s)

Sensor(s)

Physical
Process

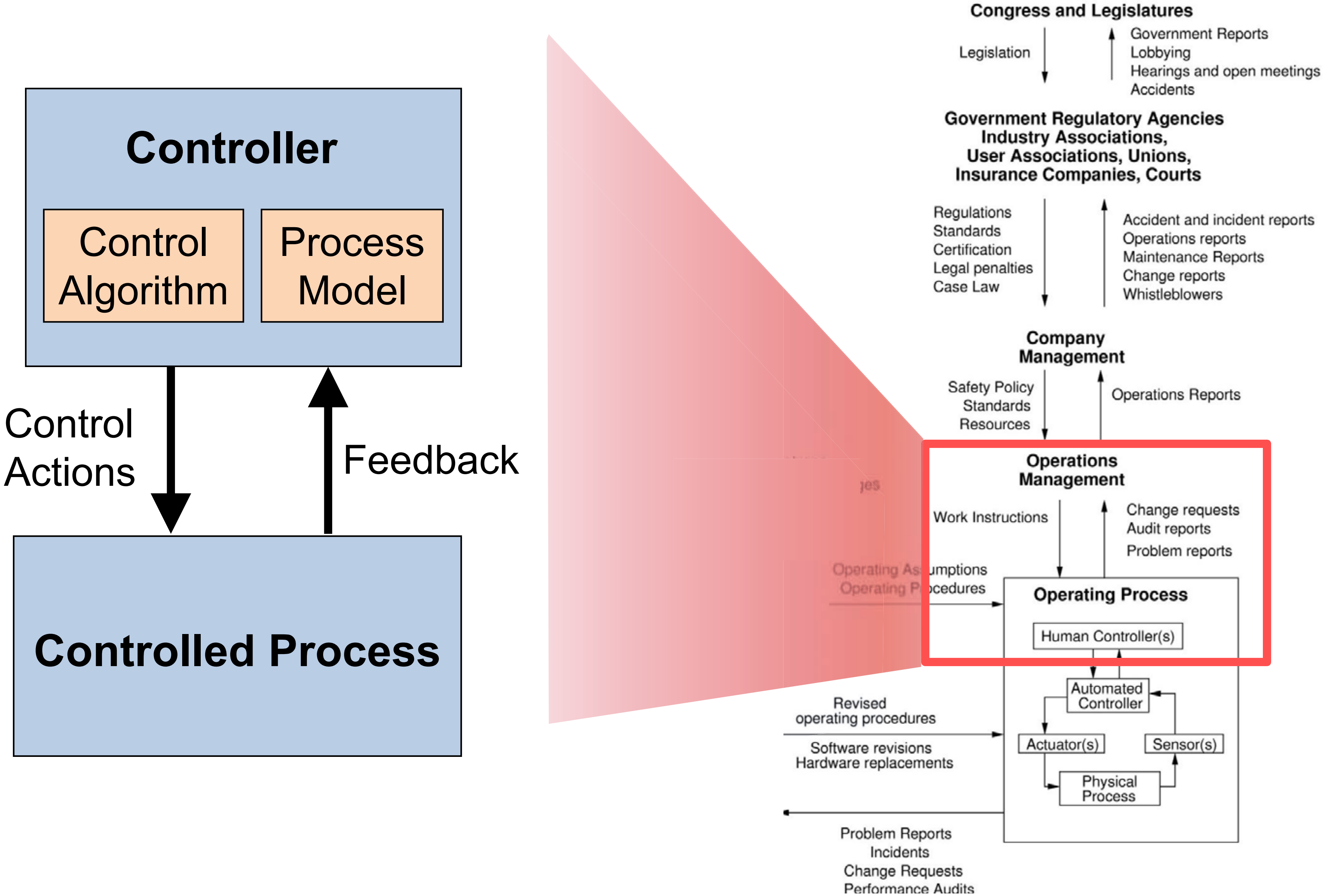
Revised
operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Using control theory



Controller

Control Algorithm

Process Model

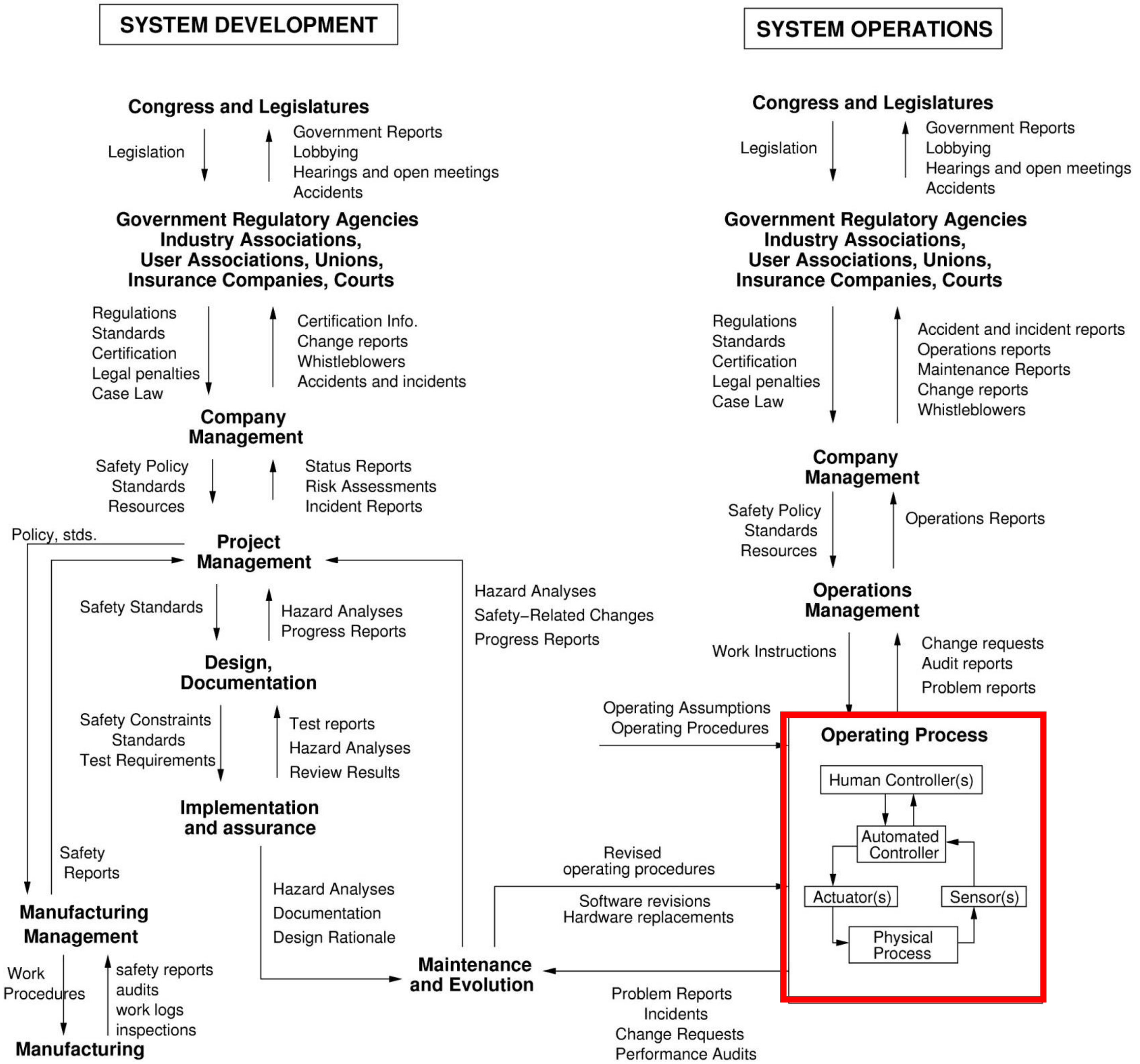
Control Actions

Feedback

Controlled Process

From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

Example Safety Control Structure



SYSTEM DEVELOPMENT

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company
Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project
Management

Safety Standards

Hazard Analyses
Progress Reports

Design,
Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation
and assurance

Safety
Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing
Management

Work
Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance
and Evolution

Hazard Analyses
Safety–Related Changes
Progress Reports

SYSTEM OPERATIONS

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company
Management

Safety Policy
Standards
Resources

Operations Reports

Operations
Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated
Controller

Actuator(s)

Sensor(s)

Physical
Process

Revised
operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

From Leveson, Nancy (2012). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology. Used with permission.

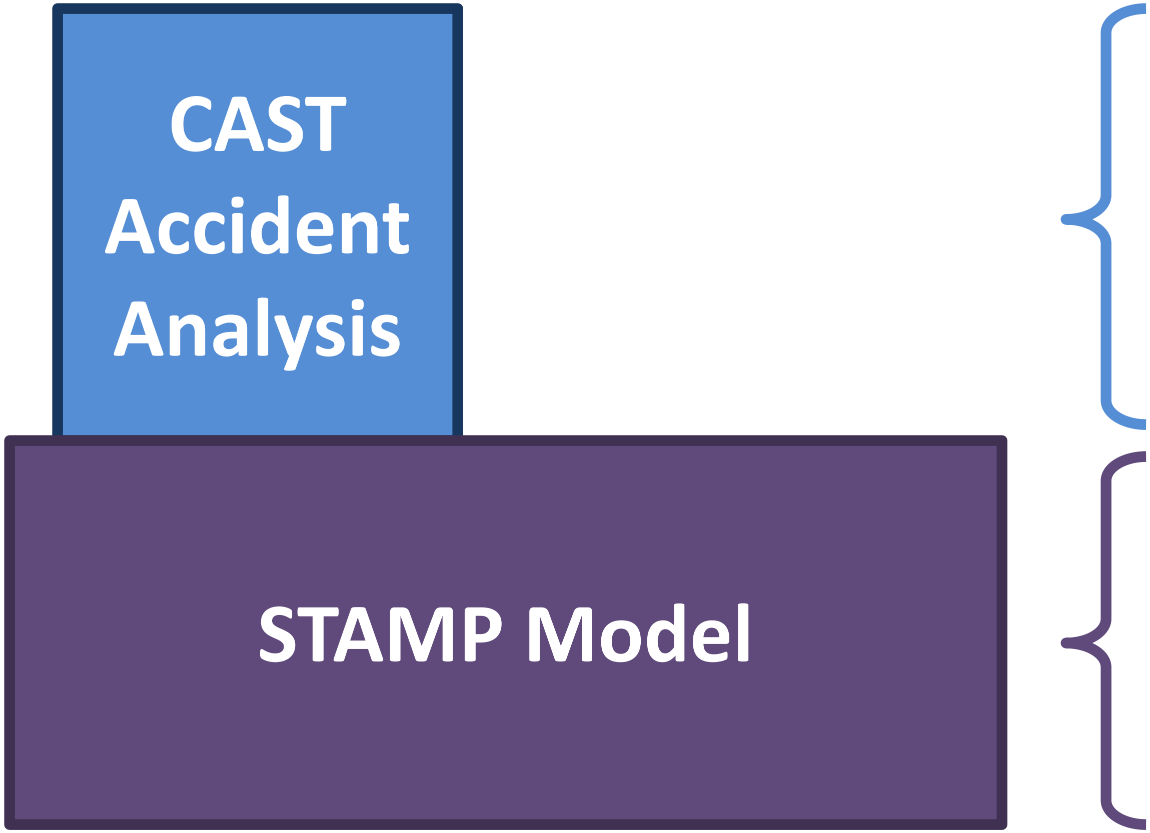
(Leveson, 2012)

STAMP and STPA

STAMP Model

Accidents are caused by inadequate control

STAMP and STPA



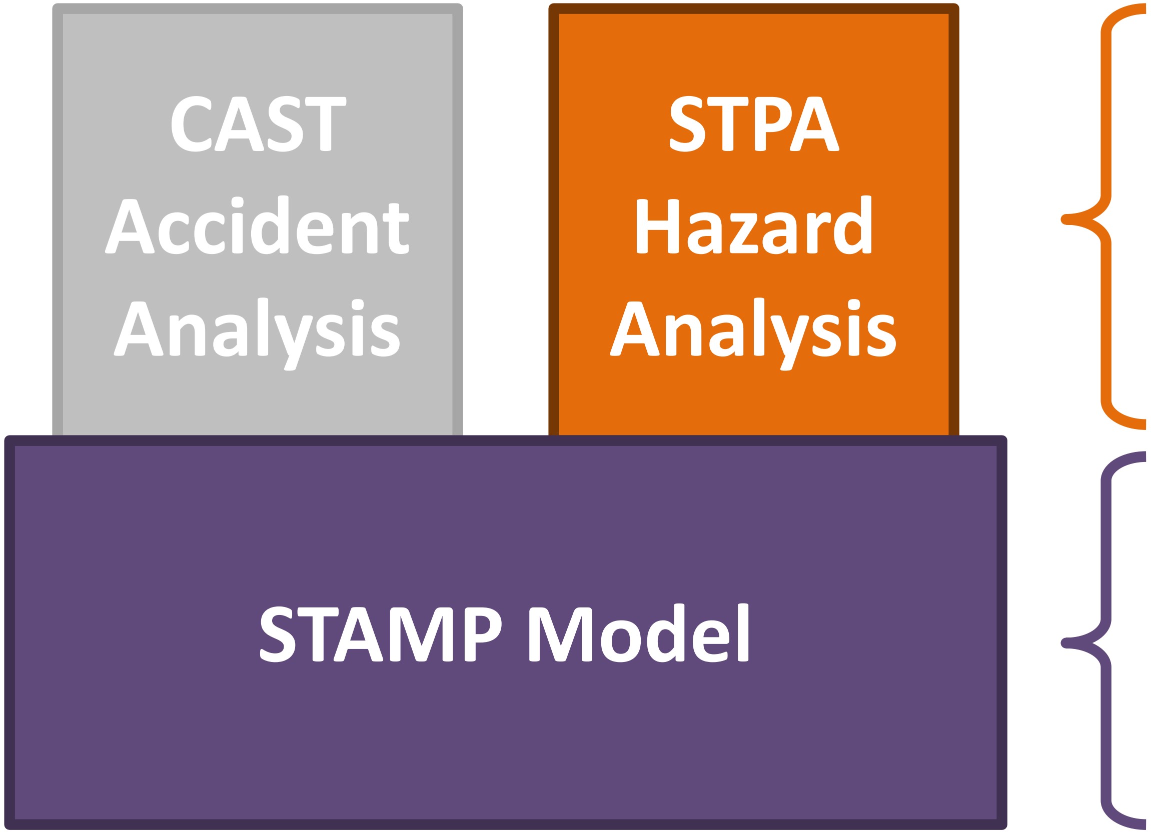
CAST Accident Analysis

STAMP Model

How do we find inadequate control that caused an accident?

Accidents are caused by inadequate control

STAMP and STPA

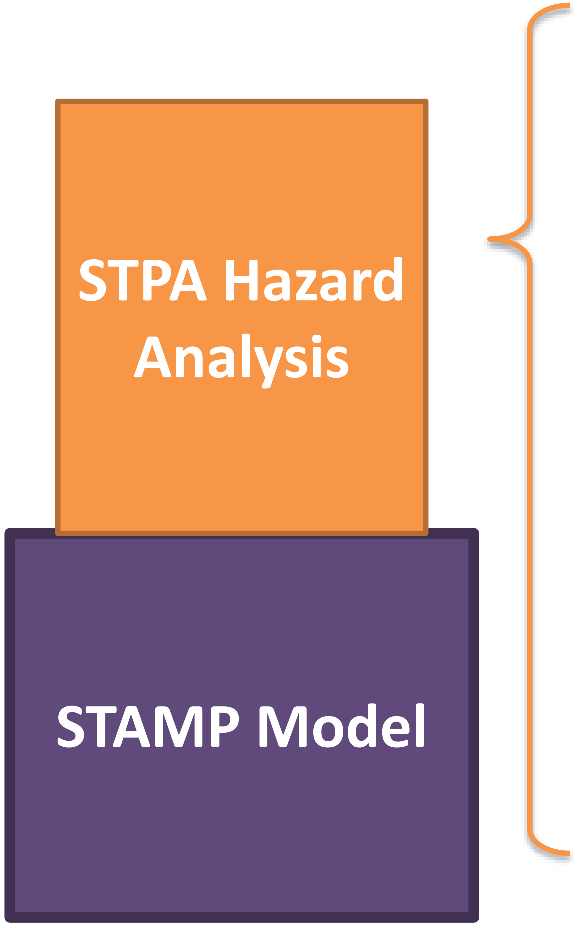


How do we find inadequate control in a design?

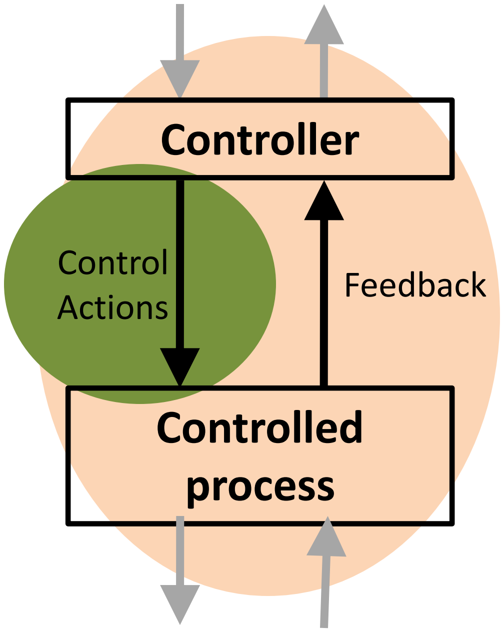
Accidents are caused by inadequate control

STPA Hazard Analysis

STPA
(System-Theoretic Process Analysis)



- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



Can capture requirements flaws, software errors, human errors

(Leveson, 2012)

Definitions

- Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

- Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).

Definitions from Engineering a Safer World

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- System Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

System Accident	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors **outside our control**
- System Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

System Accident	System Hazard
People die from exposure to toxic chemicals	Toxic chemicals from the plant are in the atmosphere
People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

Broad view of safety

“Accident” is anything that is unacceptable, that must be prevented.

Not limited to loss of life or human injury!

People die from radiation sickness	Nuclear power plant radioactive materials are not contained
Vehicle collides with another vehicle	Vehicles do not maintain safe distance from each other
People die from food poisoning	Food products for sale contain pathogens

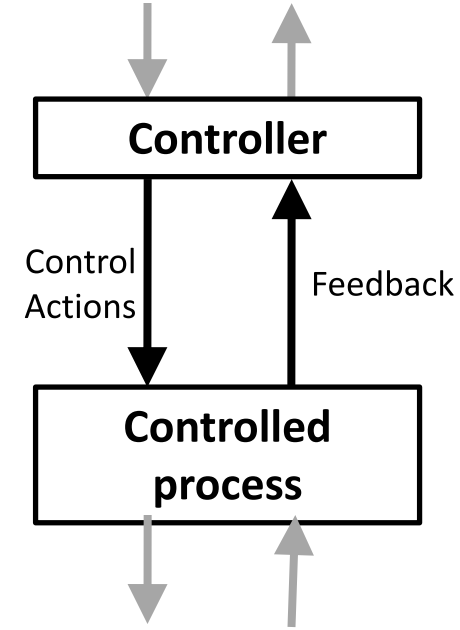
System Safety Constraints

System Hazard		System Safety Constraint
Toxic chemicals from the plant are in the atmosphere	➡	Toxic plant chemicals must not be released into the atmosphere
Nuclear power plant radioactive materials are not contained	➡	Radioactive materials must note be released
Vehicles do not maintain safe distance from each other	➡	Vehicles must always maintain safe distances from each other
Food products for sale contain pathogens	➡	Food products with pathogens must not be sold

Additional hazards / constraints can be found in ESW p355

STPA
(System-Theoretic Process Analysis)

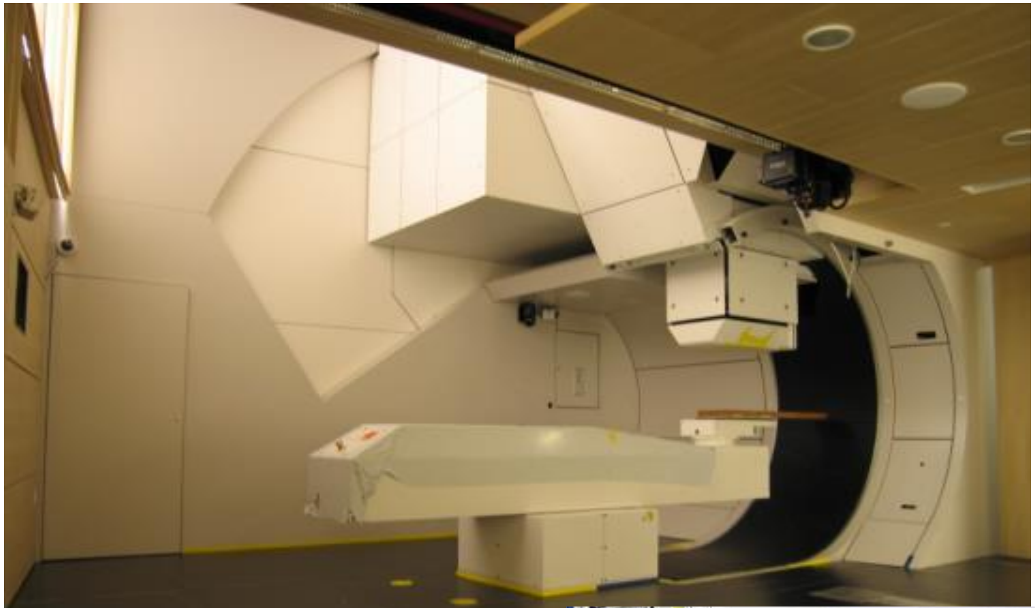
- ✓ Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



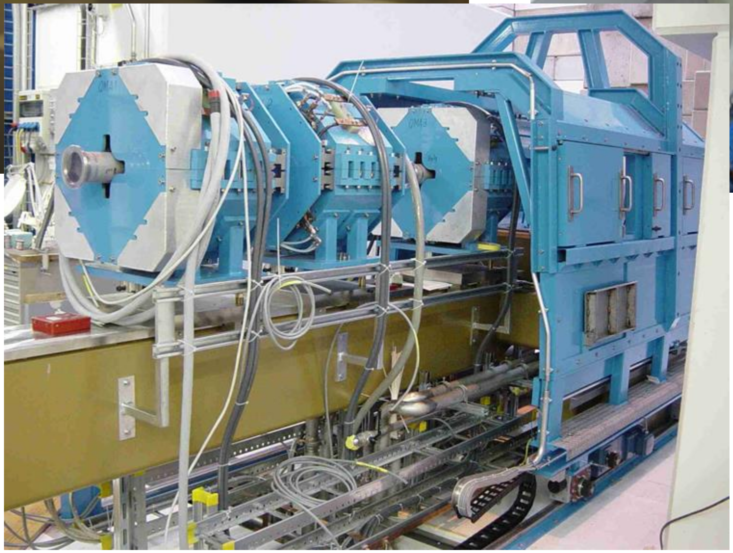
(Leveson, 2012)

Control Structure Examples

Proton Therapy Machine High-level Control Structure



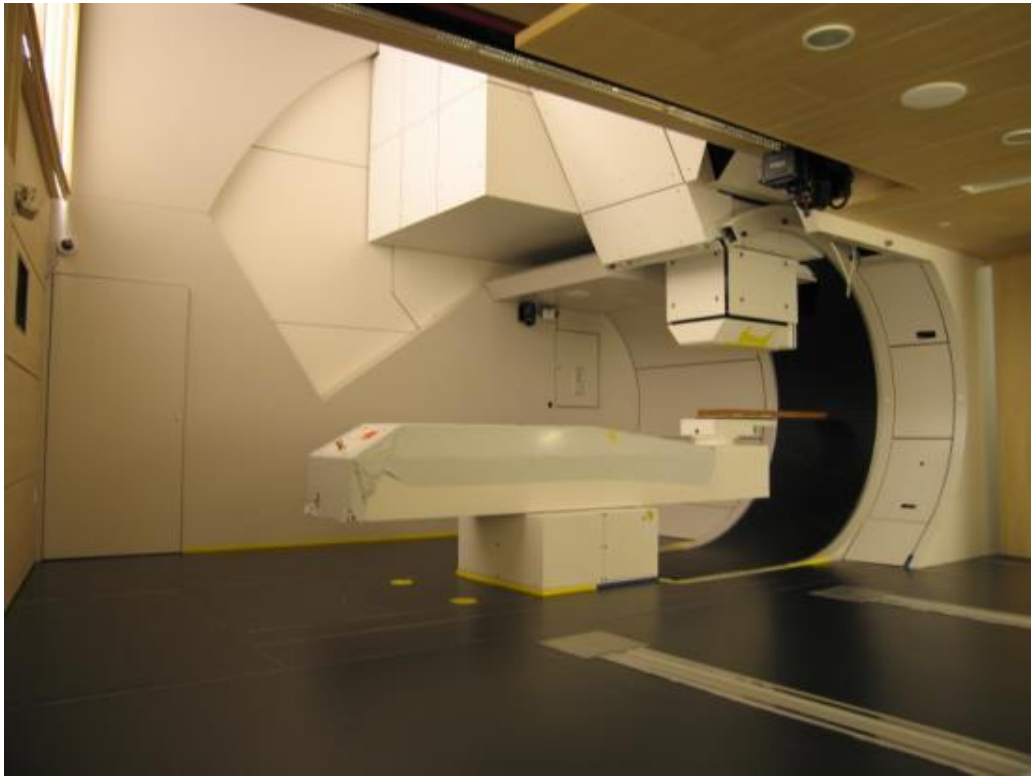
Gantry

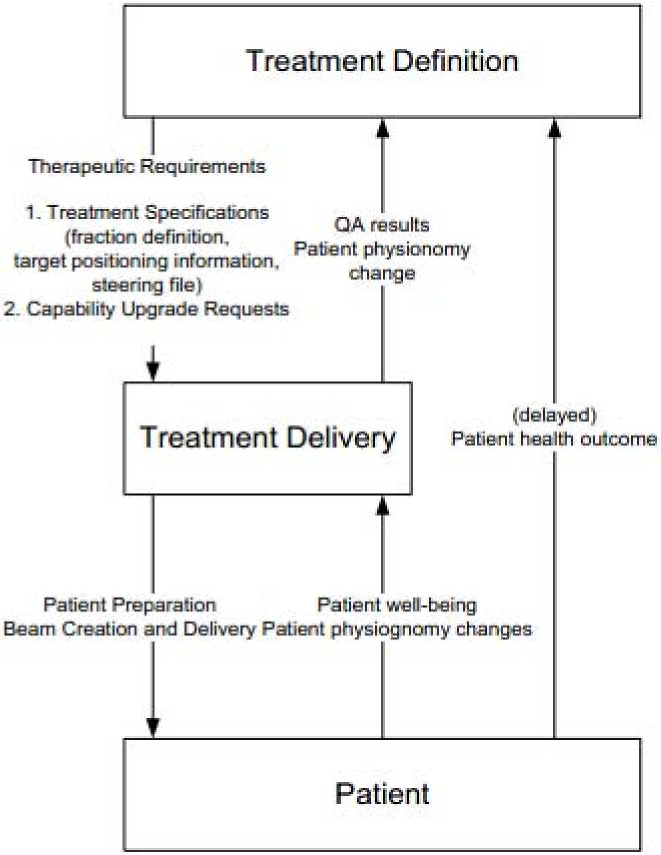


Beam path and

control elements

Proton Therapy Machine High-level Control Structure





Treatment Definition
Therapeutic Requirements
1. Treatment Specifications (fraction definition, target positioning information, steering file)
2. Capability Upgrade Requests
QA results
Patient physionomy change
Treatment Delivery
(delayed) Patient health outcome
Patient Preparation
Beam Creation and Delivery
Patient well-being
Patient physiognomy changes
Patient

Figure 11 - High-level functional description of the PROSCAN facility (D0)

Courtesy of MIT. Used with permission.

Antoine PhD Thesis, 2012

Proton Therapy Machine Control Structure

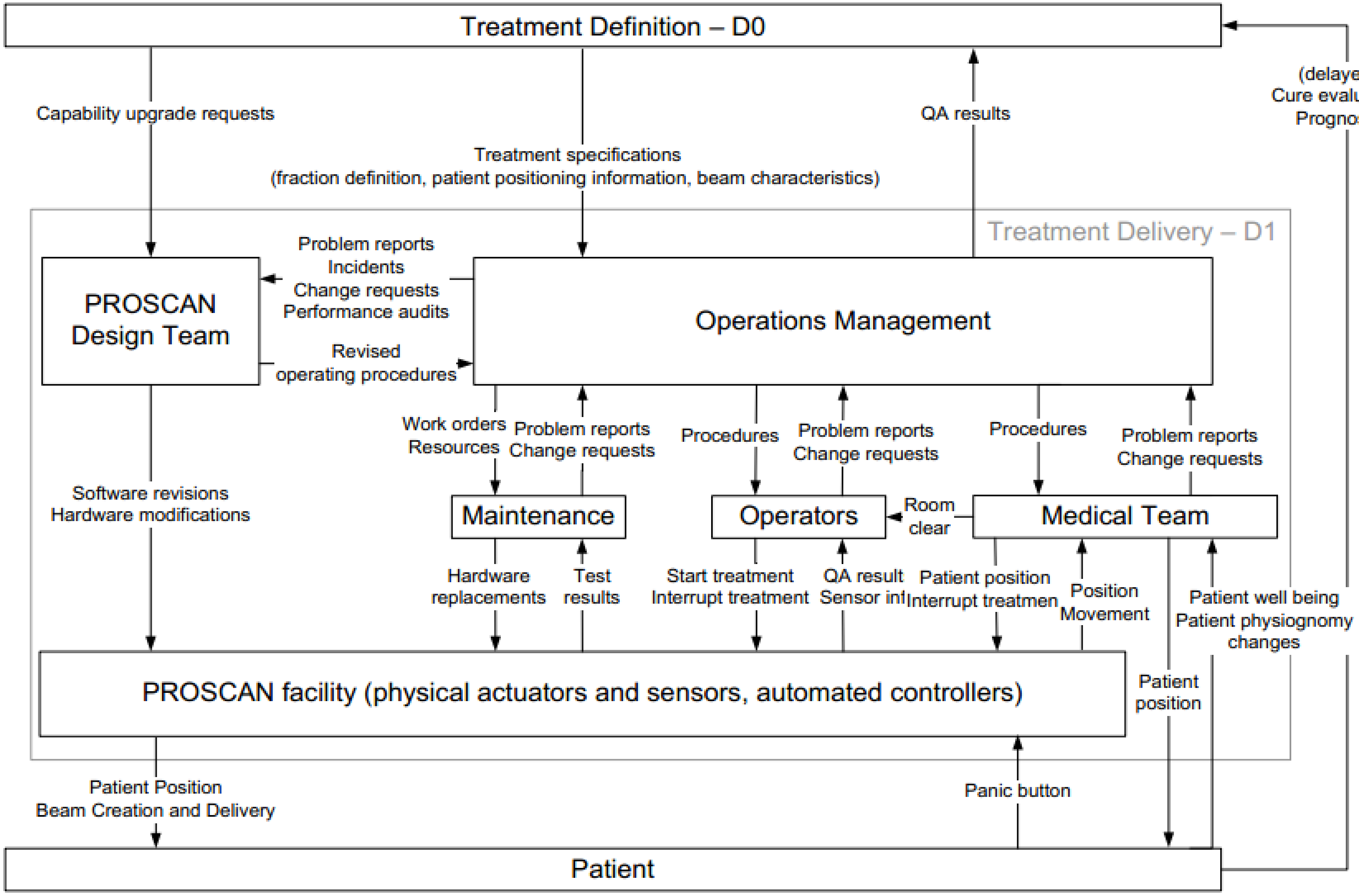


Figure 13 - Zooming into the Treatment Delivery group (D1)

Courtesy of MIT. Used with permission.

Antoine PhD Thesis, 2012

Adaptive Cruise Control

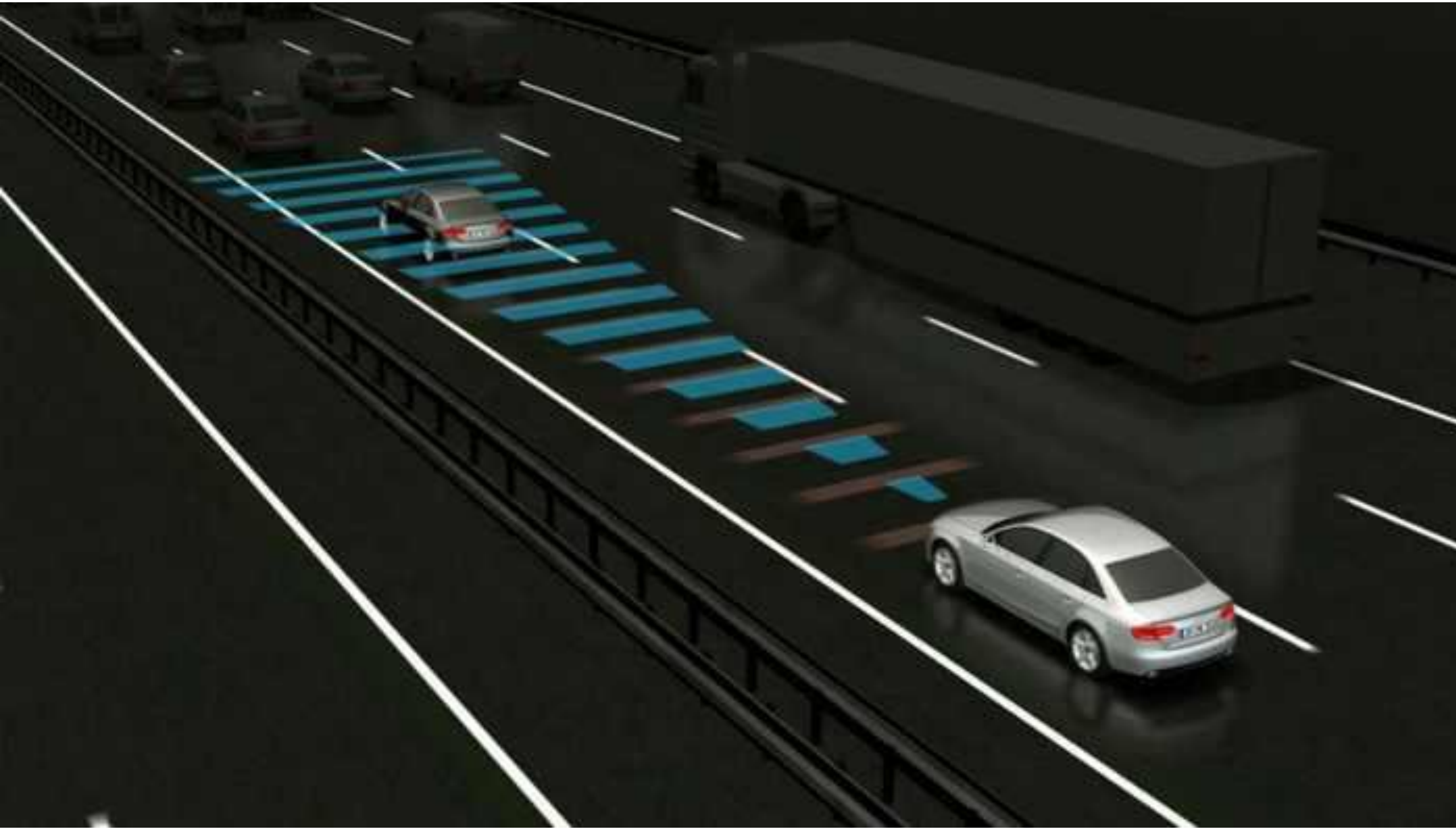
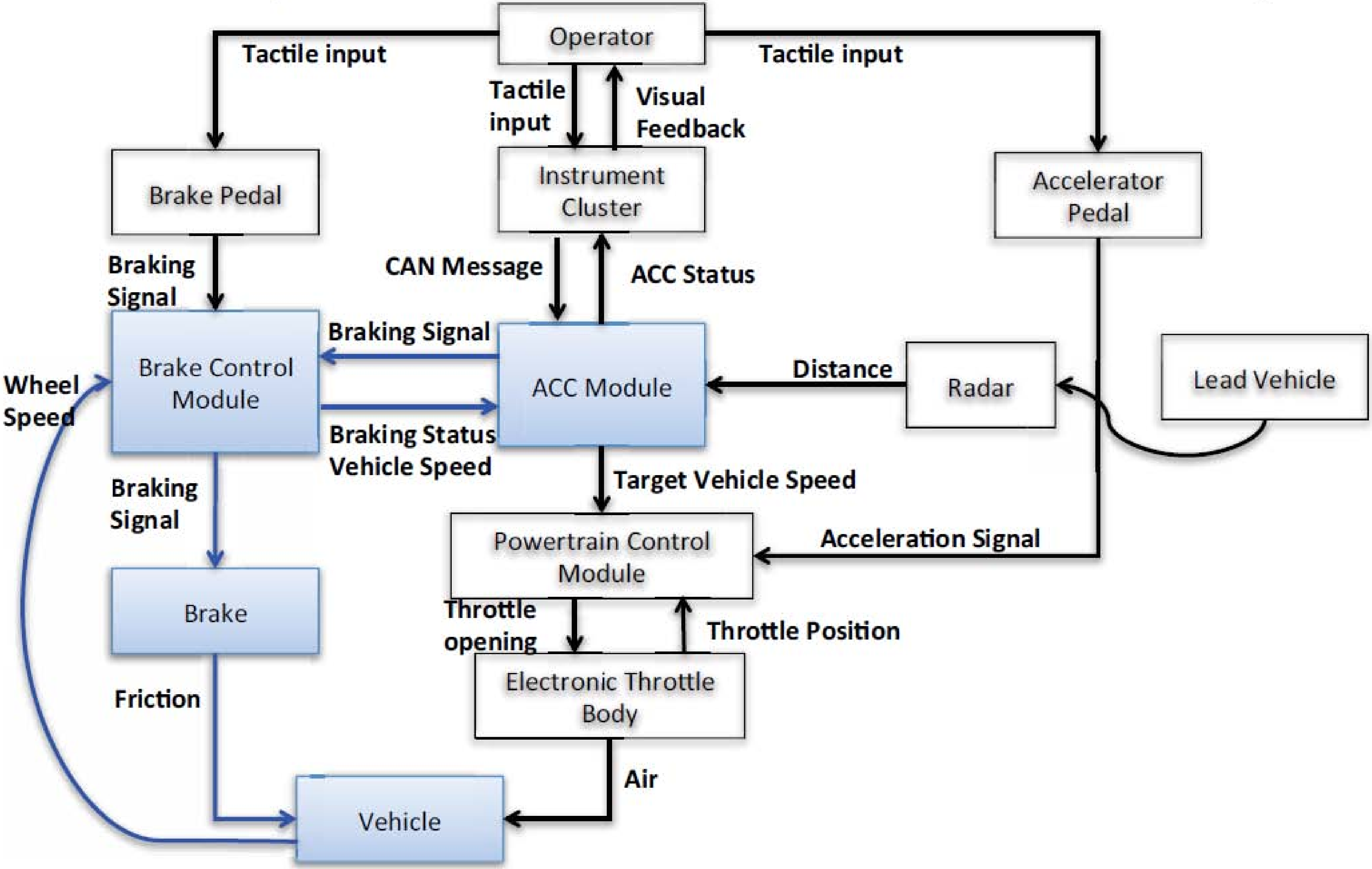


Image from: http://www.audi.com/etc/medialib/ngw/efficiency/video_assets/fallback_videos.Par.0002.Image.jpg

Example: ACC – BCM Control Loop



Courtesy of Qi D. Van Eikema Hommes. Used with permission.

Chemical Plant

An image of the explosion at the Bayer chemical plant in Institute, West Virginia removed due to copyright restrictions.

Image from: http://www.cbgnetwork.org/2608.html

Chemical Plant

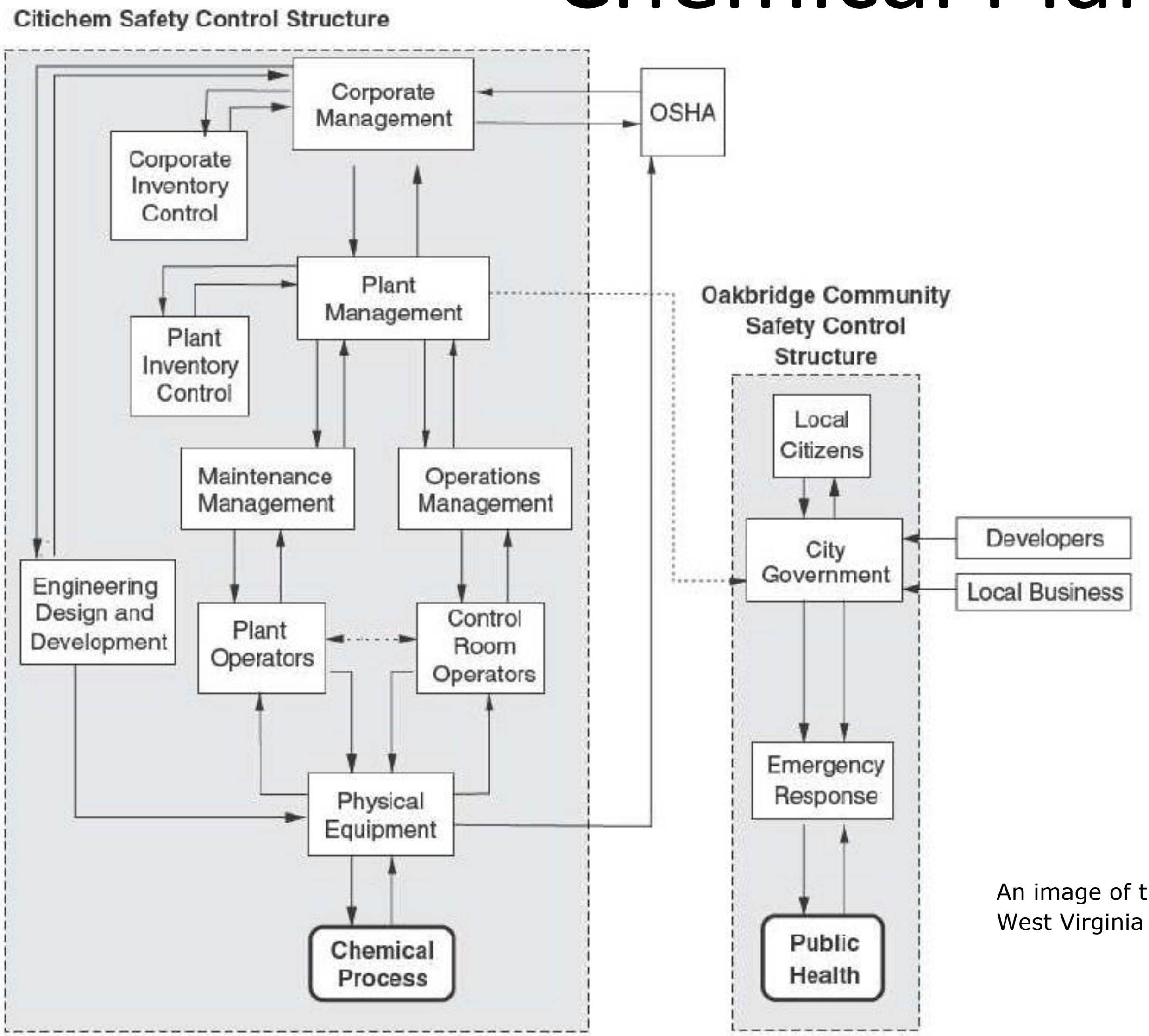


Image from: http://www.cbgnetwork.org/2608.html

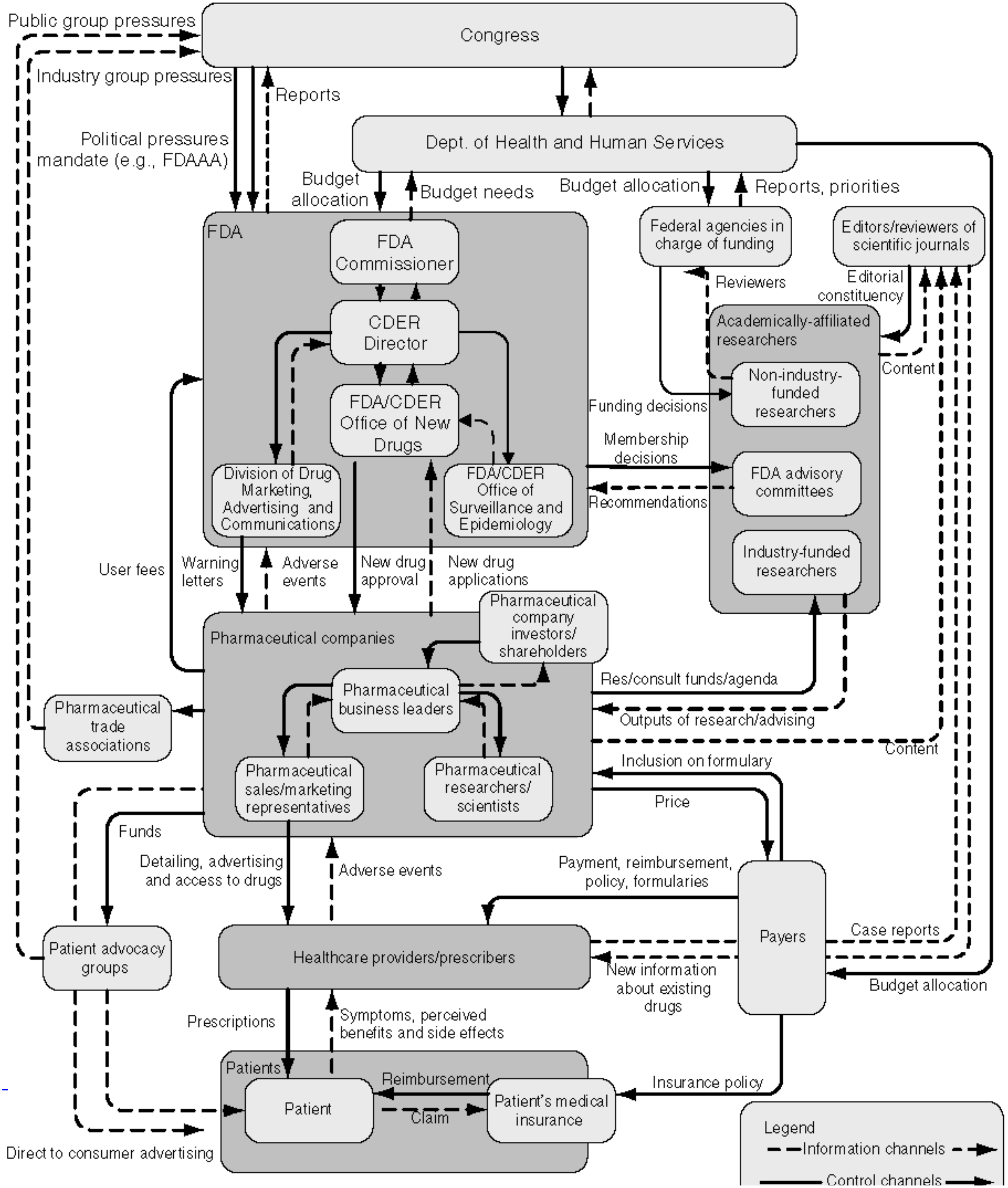
An image of the explosion at the Bayer chemical plant in Institute, West Virginia removed due to copyright restrictions.

ESW p354

U.S. pharmaceutical safety control structure

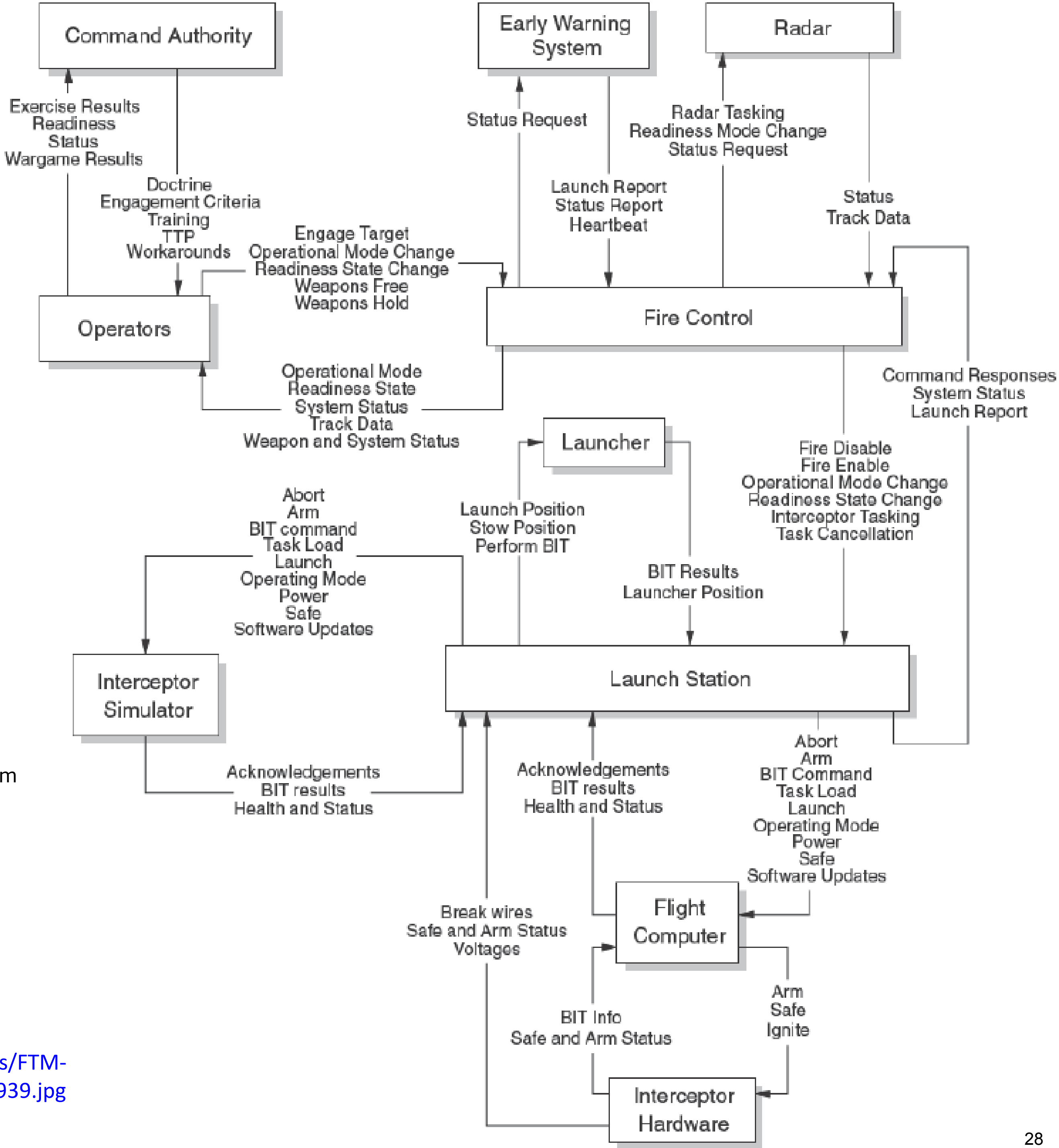
An image of the prescription drug Vioxx removed due to copyright restrictions.

Image from: http://www.kleantreatmentcenter.com/wp-content/uploads/2012/07/vioxx.jpeg



Public group pressures
Congress
Industry group pressures
Reports
Political pressures mandate (e.g., FDAAA)
Dept. of Health and Human Services
Budget allocation
Budget needs
Budget allocation
Reports, priorities
FDA
FDA Commissioner
Federal agencies in charge of funding
Editors/reviewers of scientific journals
Reviewers
Editorial constituency
CDER Director
Academically-affiliated researchers
Content
Non-industry-funded researchers
FDA/CDER Office of New Drugs
Funding decisions
Membership decisions
FDA advisory committees
Recommendations
Division of Drug Marketing, Advertising and Communications
FDA/CDER Office of Surveillance and Epidemiology
Industry-funded researchers
User fees
Warning letters
Adverse events
New drug approval
New drug applications
Pharmaceutical company investors/ shareholders
Pharmaceutical companies
Res/consult funds/agenda
Pharmaceutical business leaders
Outputs of research/advising
Pharmaceutical trade associations
Content
Inclusion on formulary
Pharmaceutical sales/marketing representatives
Pharmaceutical researchers/ scientists
Price
Funds
Detailing, advertising and access to drugs
Adverse events
Payment, reimbursement, policy, formularies
Patient advocacy groups
Healthcare providers/prescribers
Payers
Case reports
New information about existing drugs
Budget allocation
Prescriptions
Symptoms, perceived benefits and side effects
Patients
Reimbursement
Patient
Claim
Patient's medical insurance
Insurance policy
Direct to consumer advertising
Legend
Information channels
Control channels

Ballistic Missile Defense System



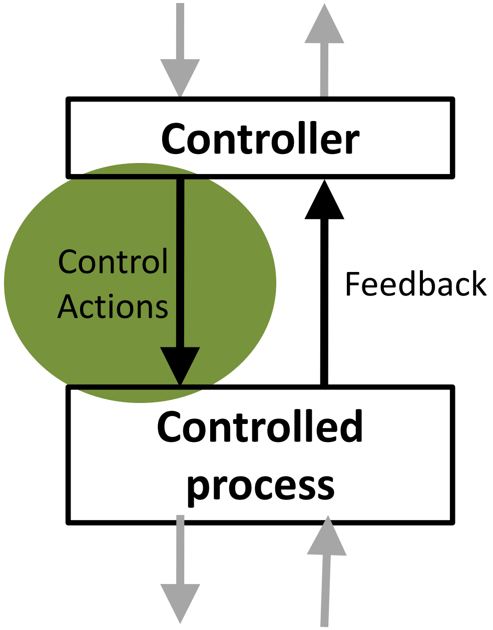
An image of the ballistic missile defense system removed due to copyright restrictions.

Image from:
http://www.mda.mil/global/images/system/aegis/FTM-21_Missile%201_Bulkhead%20Center14_BN4H0939.jpg

Safeware Corporation

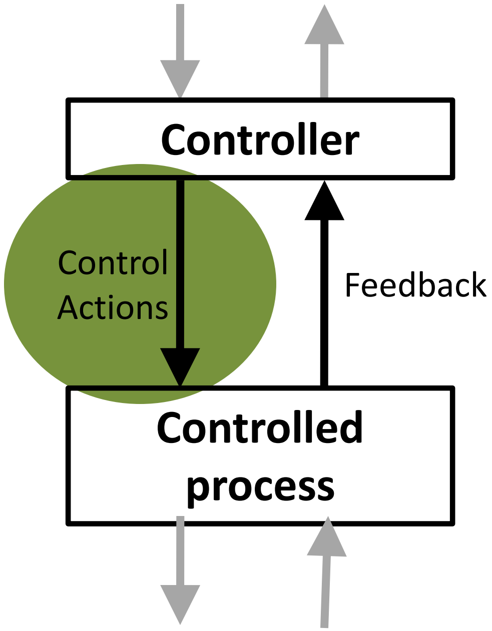
STPA
(System-Theoretic Process Analysis)

- ✓ Identify accidents and hazards
- ✓ Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios



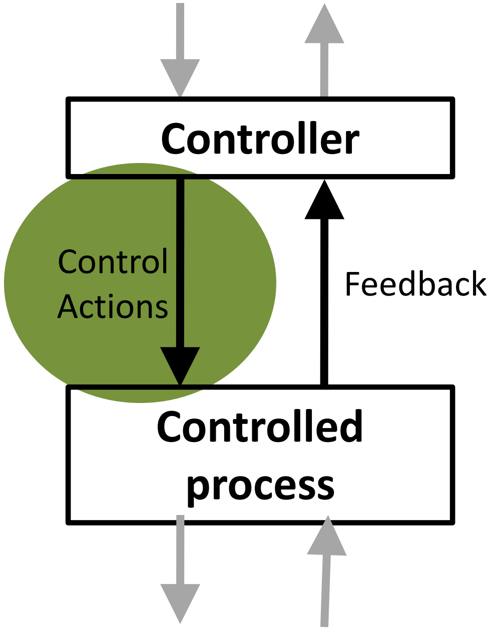
(Leveson, 2012)

STPA Step 1: Unsafe Control Actions (UCA)



Control Action A				

STPA Step 1: Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
(Control Action)				

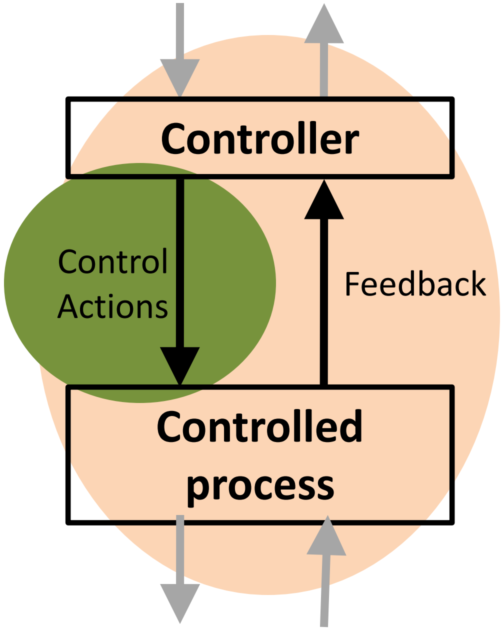
Step 1: Identify Unsafe Control Actions

(a more rigorous approach)

Control Action	Process Model Variable 1	Process Model Variable 2	Process Model Variable 3	Hazardous?

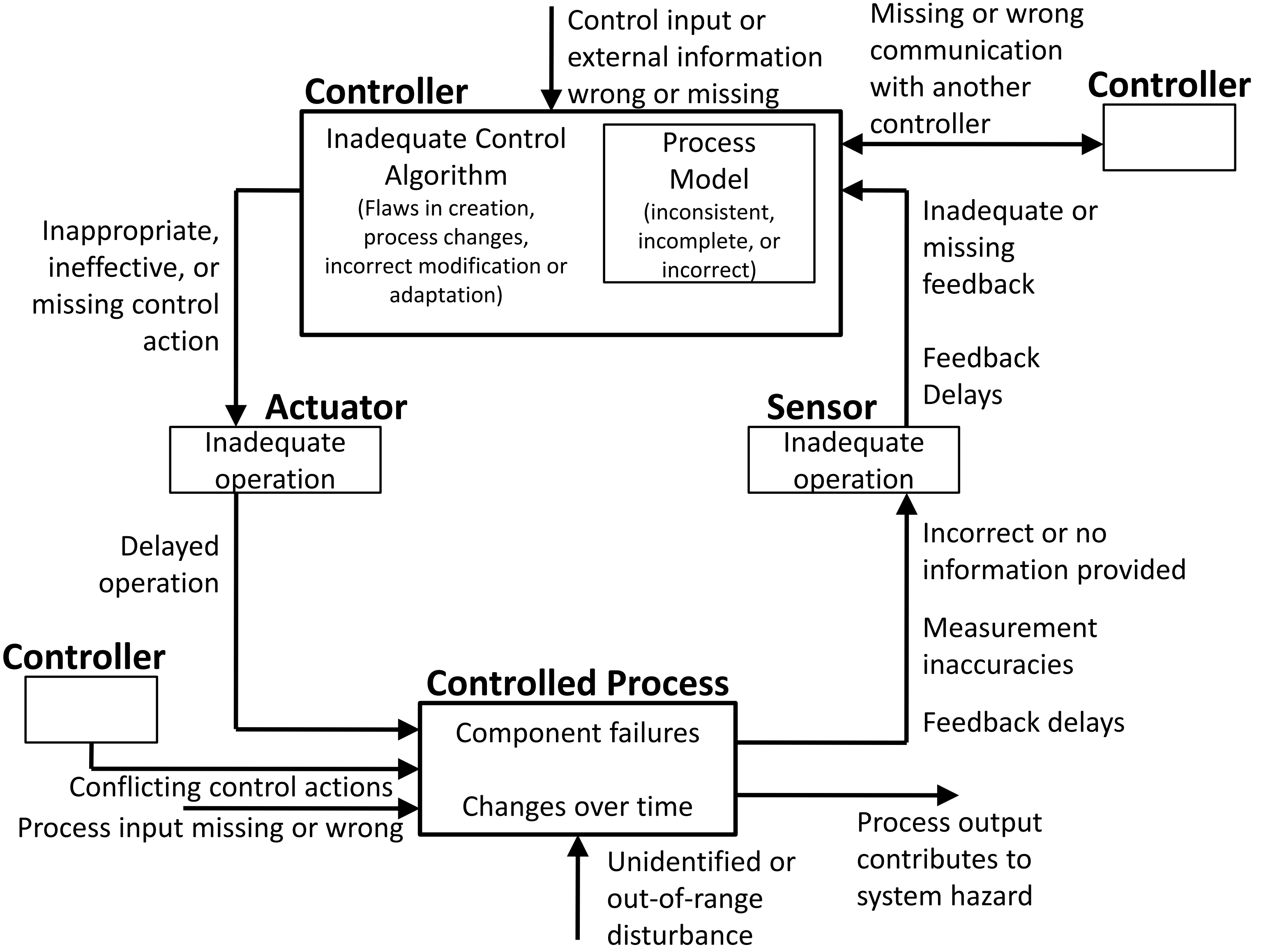
STPA
(System-Theoretic Process Analysis)

- ✓ Identify accidents and hazards
- ✓ Draw the control structure
- ✓ Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

STPA Step 2: Identify Control Flaws



Control input or external information wrong or missing

Missing or wrong communication with another controller

Controller

Controller

Inadequate Control Algorithm

(Flaws in creation, process changes, incorrect modification or adaptation)

Process Model

(inconsistent, incomplete, or incorrect)

Inappropriate, ineffective, or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Delayed operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Conflicting control actions

Process input missing or wrong

Unidentified or out-of-range disturbance

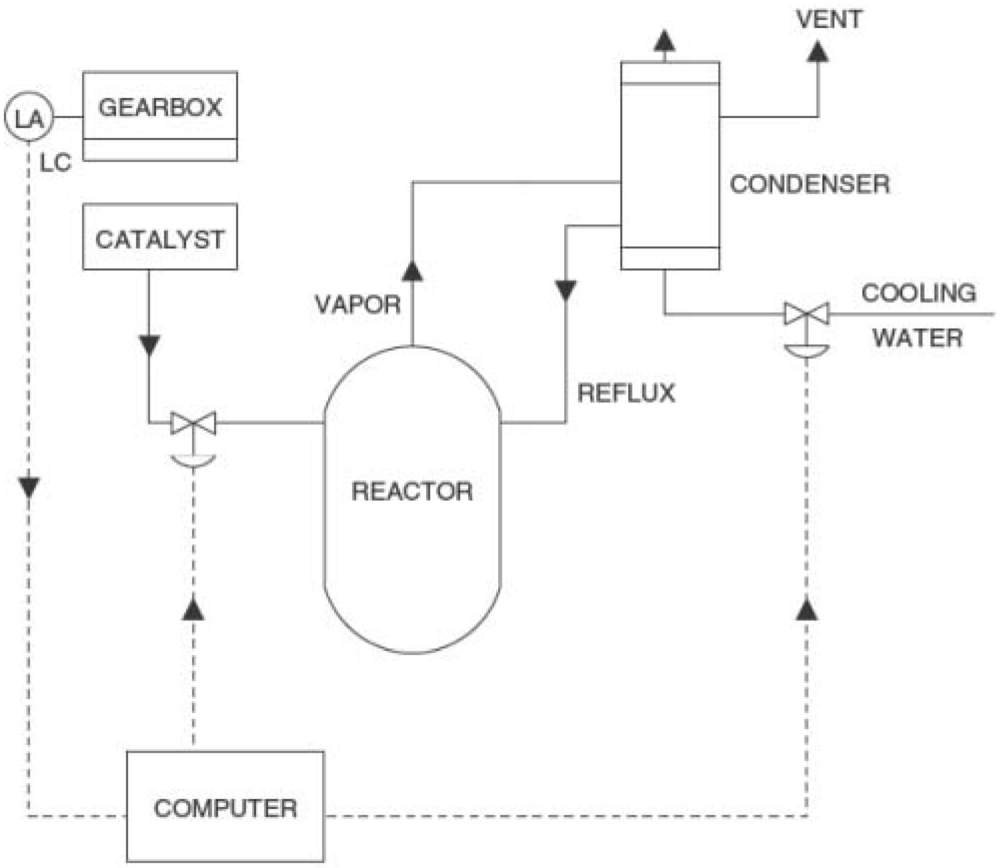
Process output contributes to system hazard

STPA Examples

Chemical Reactor

Chemical Reactor Design

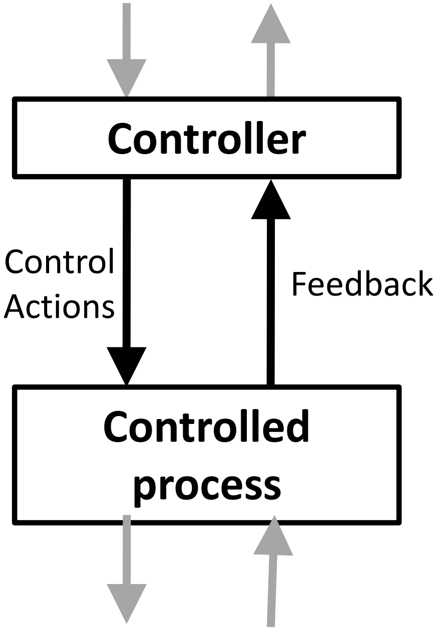
- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling



What are the accidents, system hazards, system safety constraints?

STPA
(System-Theoretic Process Analysis)

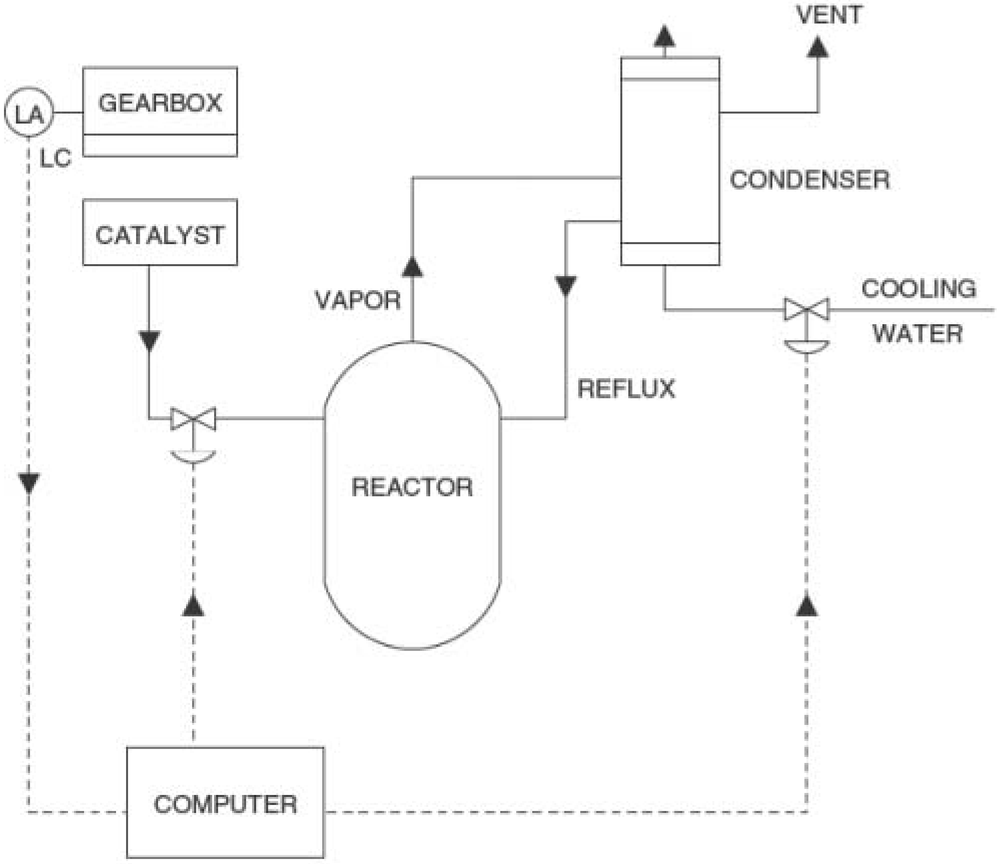
- ✓ Identify accidents and hazards
- ➡ Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

Chemical Reactor Design

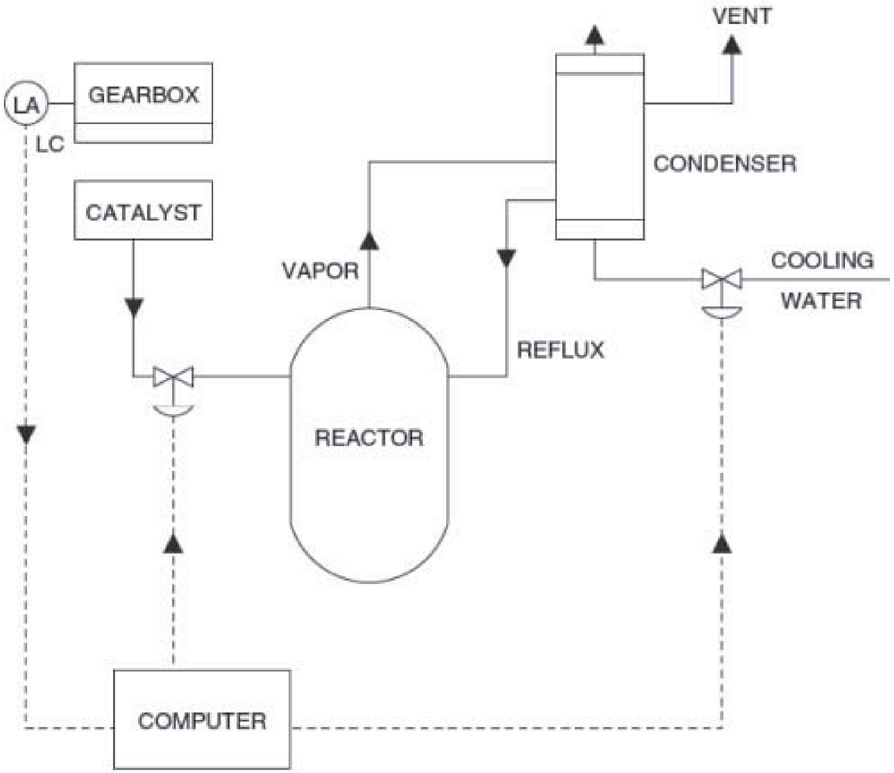
- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

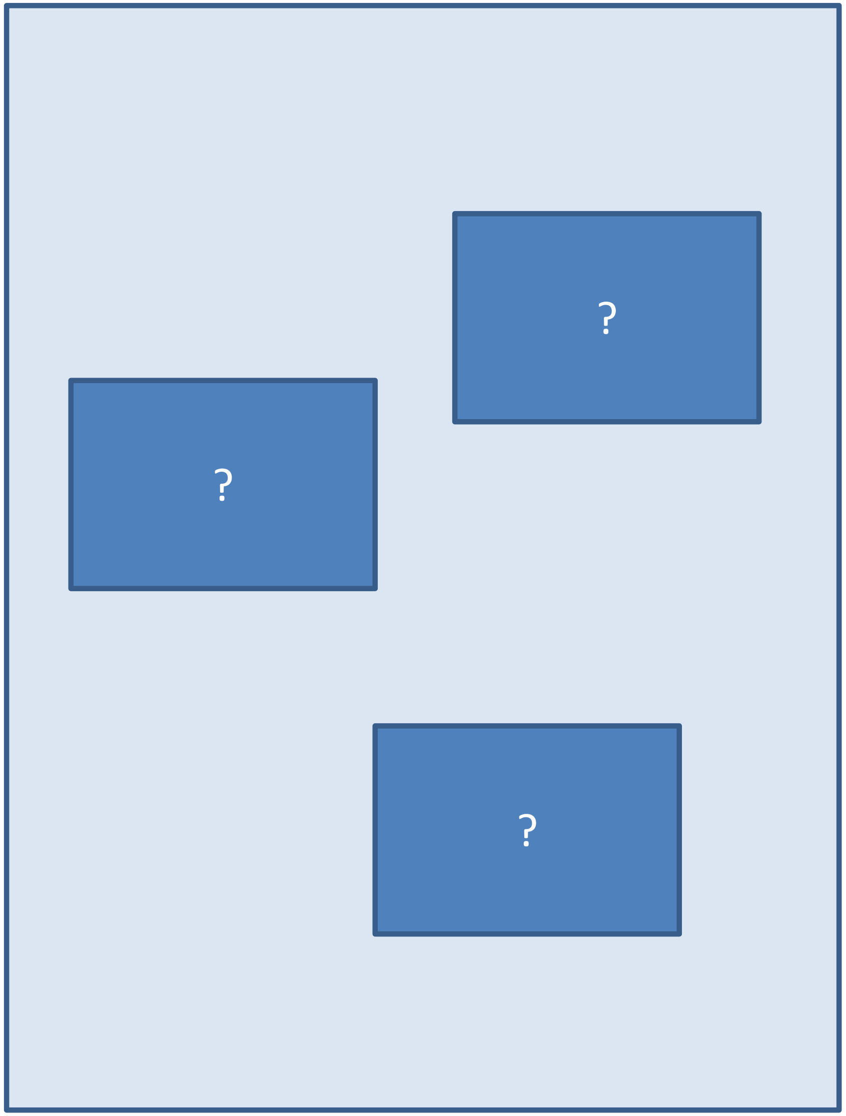


Create Control Structure

STPA Analysis

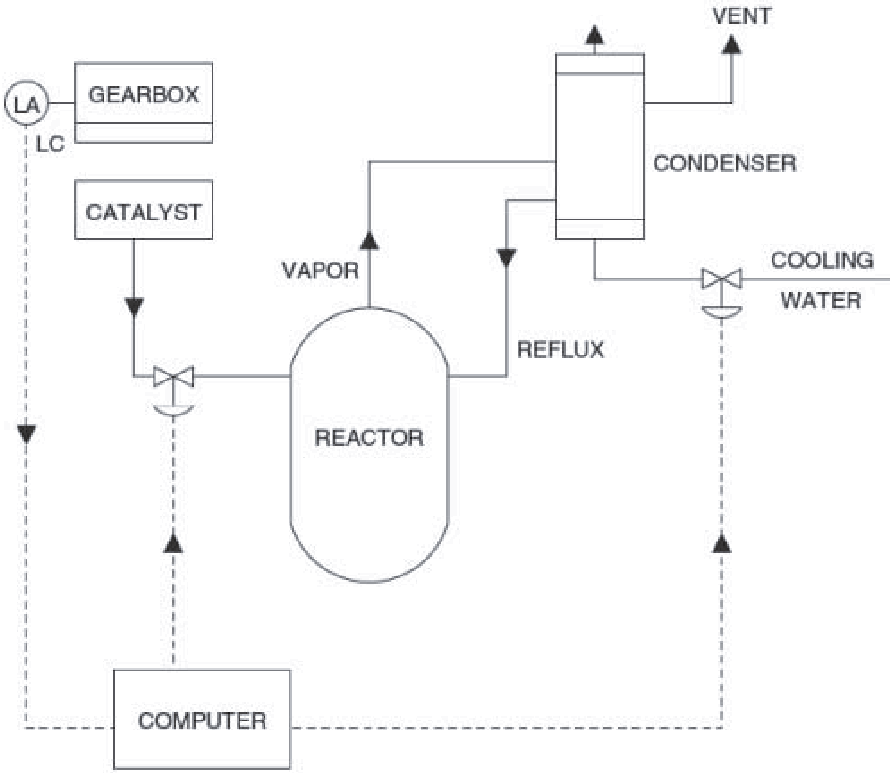
- High-level (simple) Control Structure
  - What are the main parts?

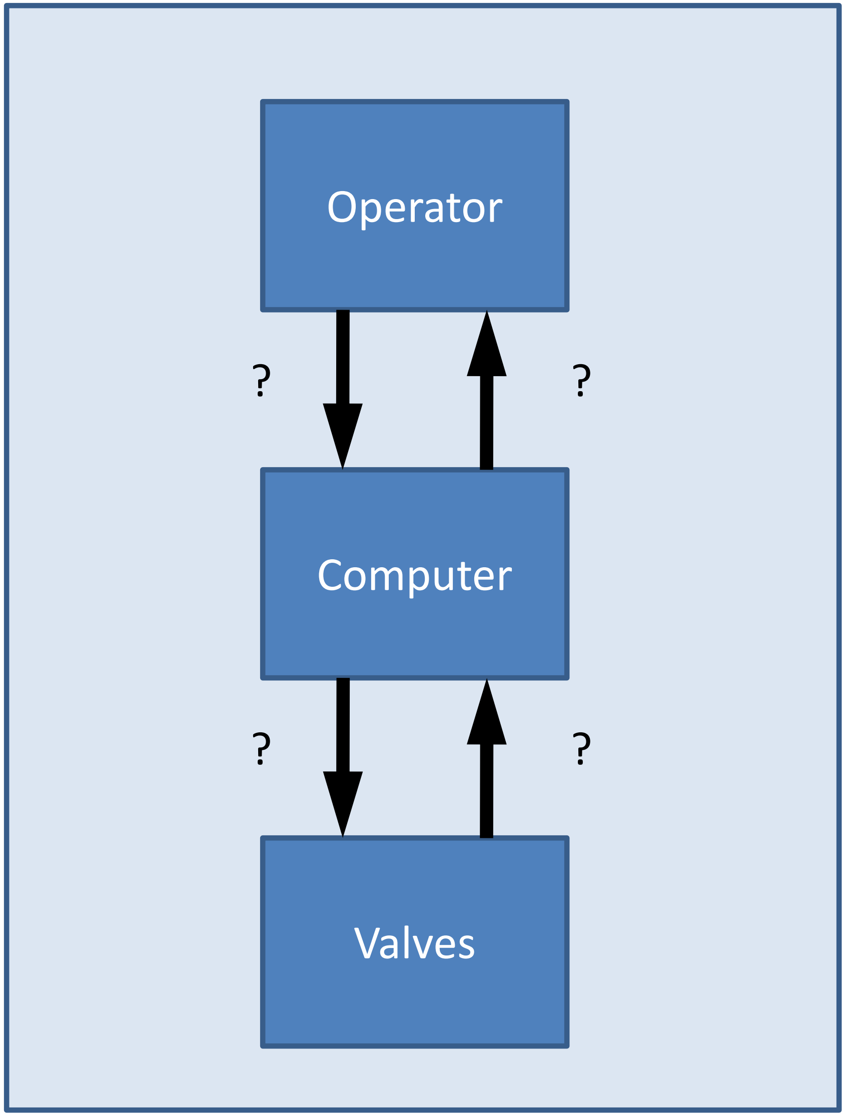




STPA Analysis

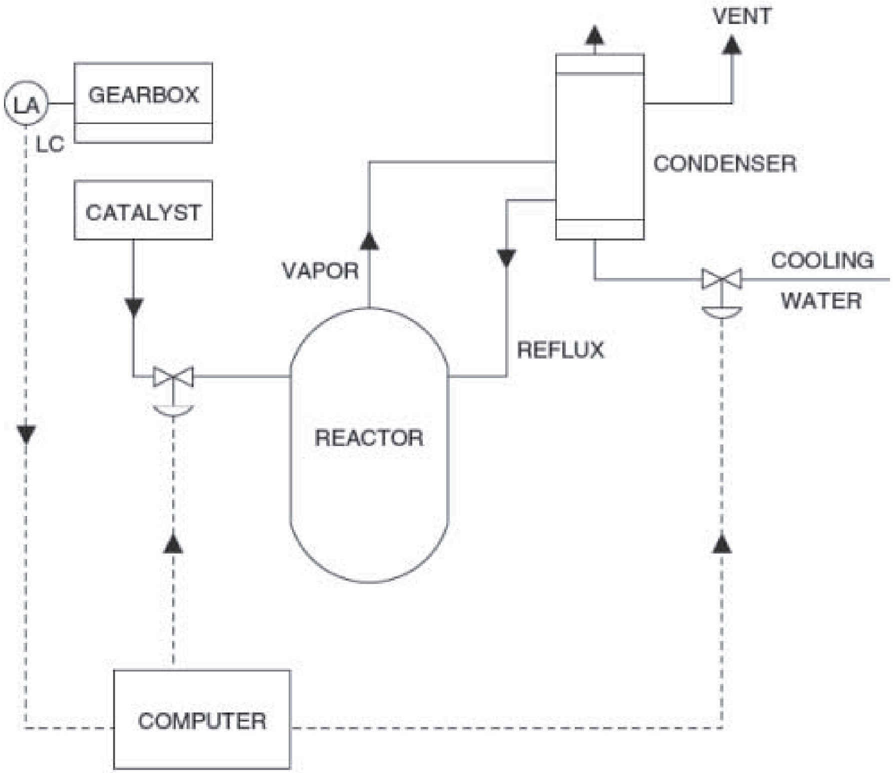
- High-level (simple) Control Structure
  - What commands are sent?

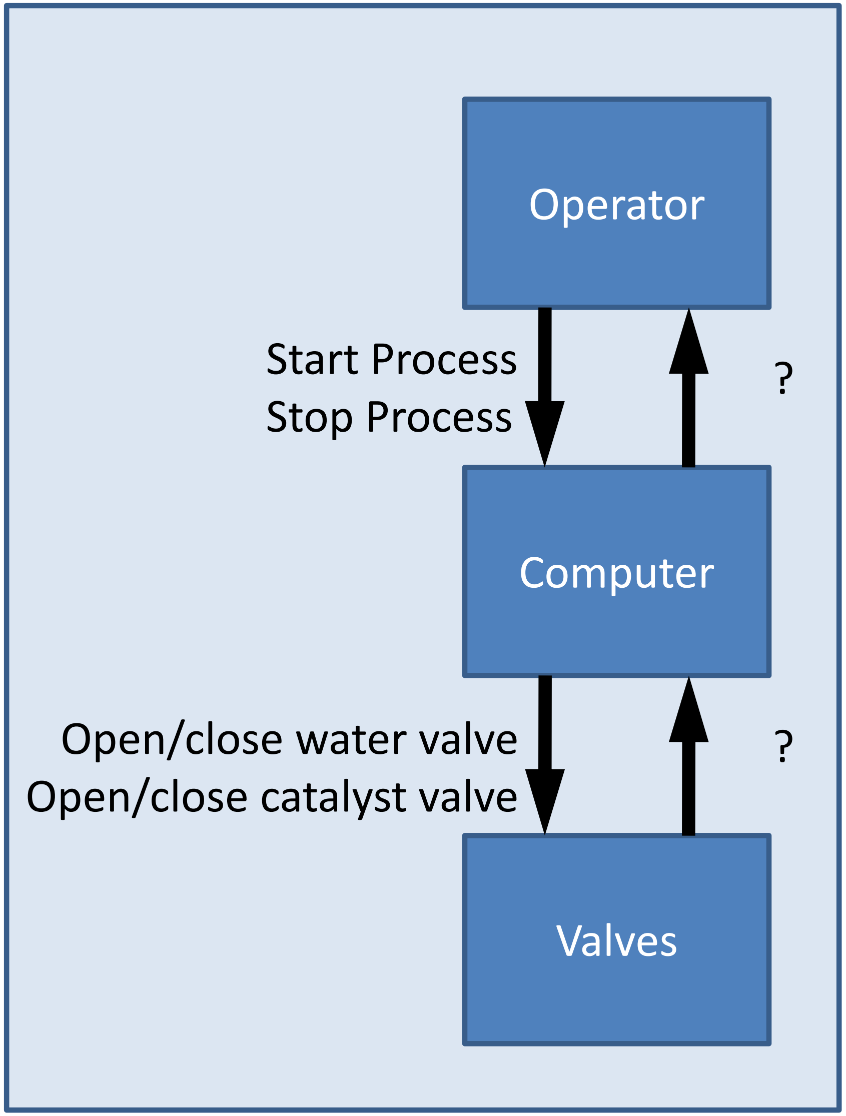




STPA Analysis

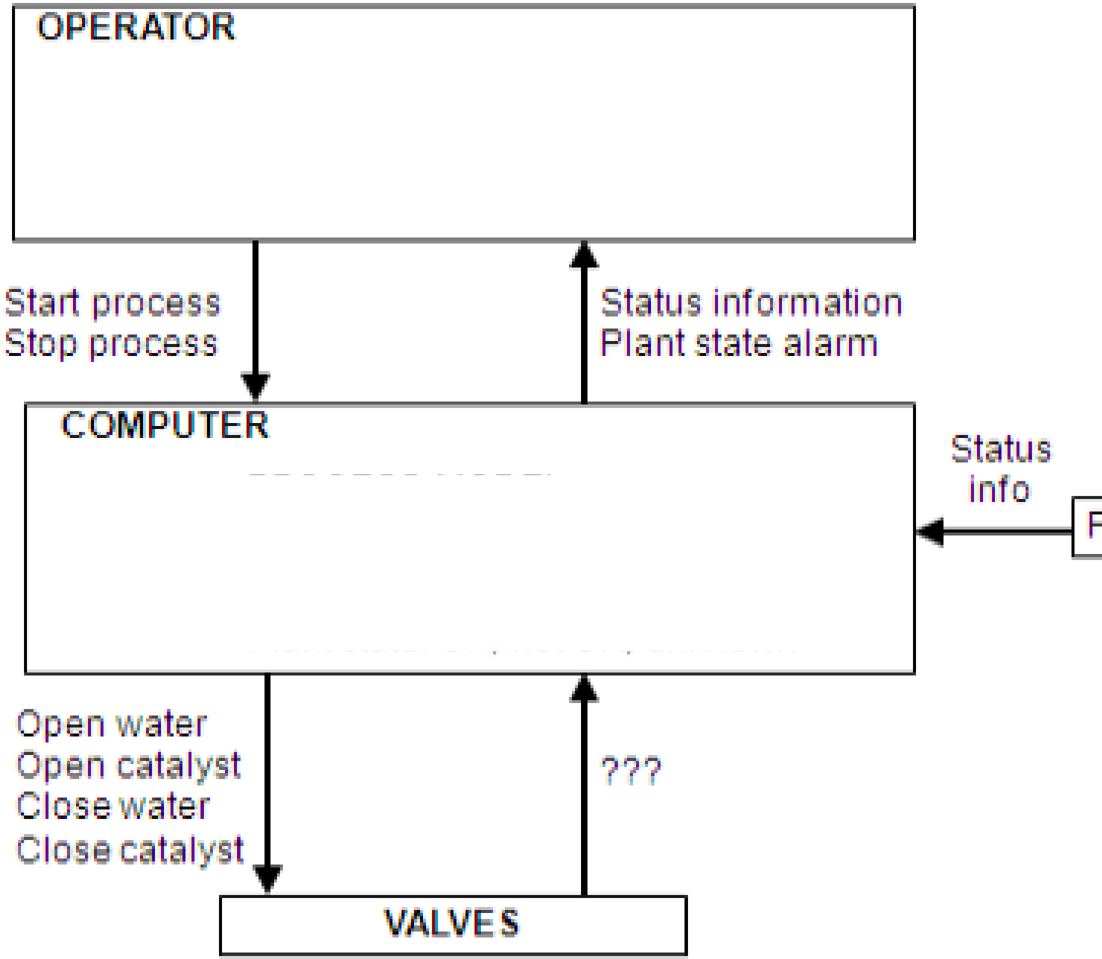
- High-level (simple) Control Structure
  - What feedback is received?





Chemical Reactor Design

Control Structure:



OPERATOR

Start process
Stop process

Status information
Plant state alarm

COMPUTER

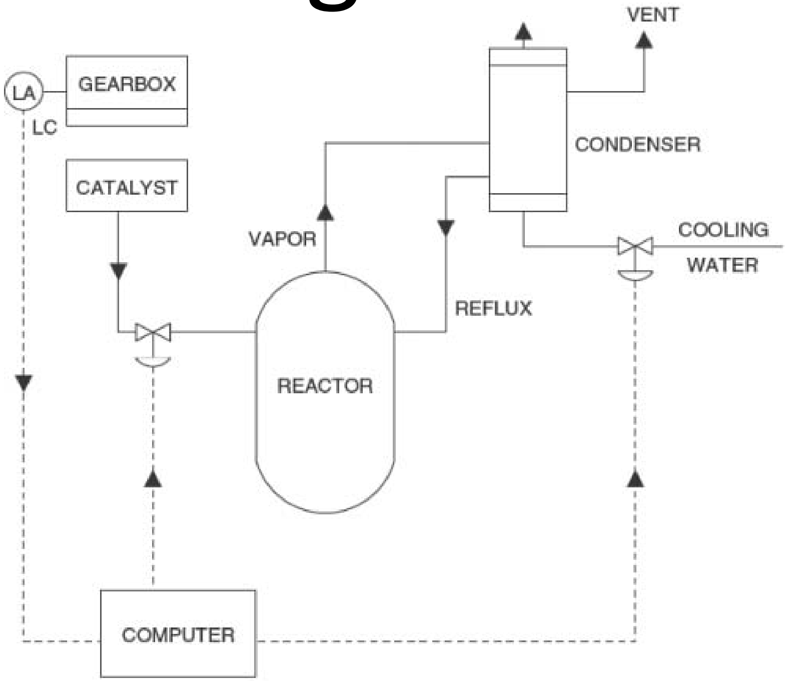
Status info

Plant

Open water
Open catalyst
Close water
Close catalyst

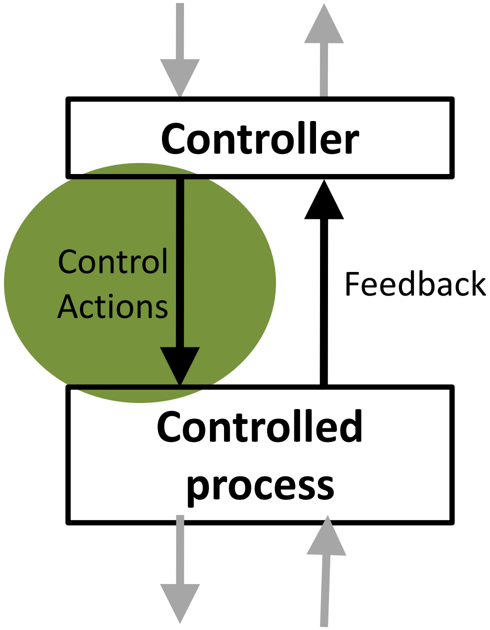
???

VALVES



STPA
(System-Theoretic Process Analysis)

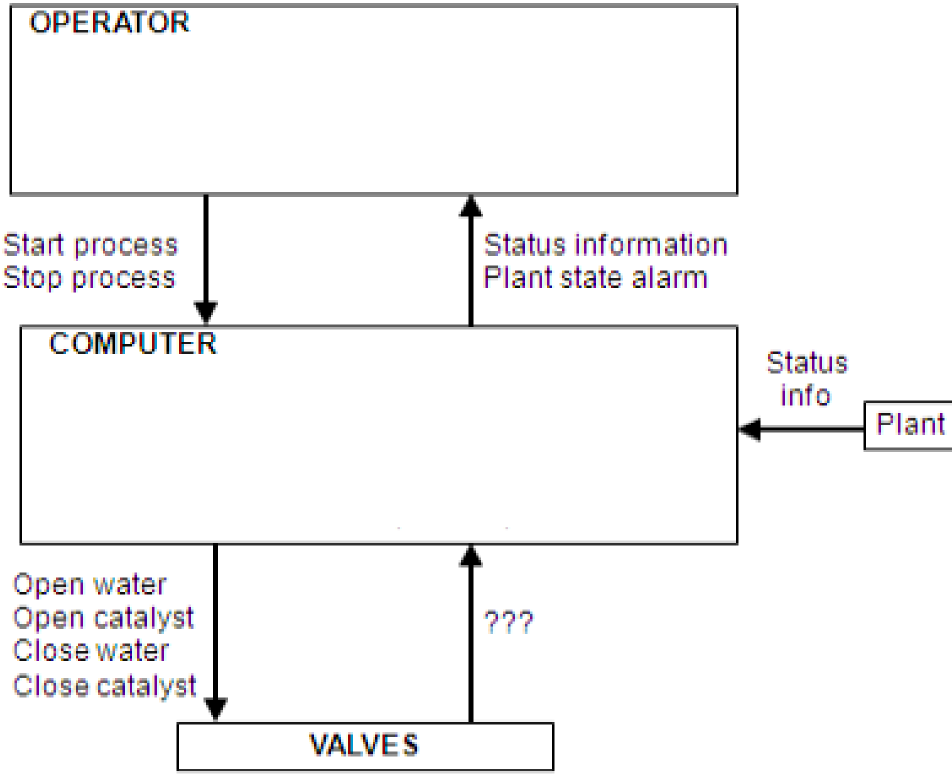
- ✓ Identify accidents and hazards
- ✓ Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

Chemical Reactor: Unsafe Control Actions

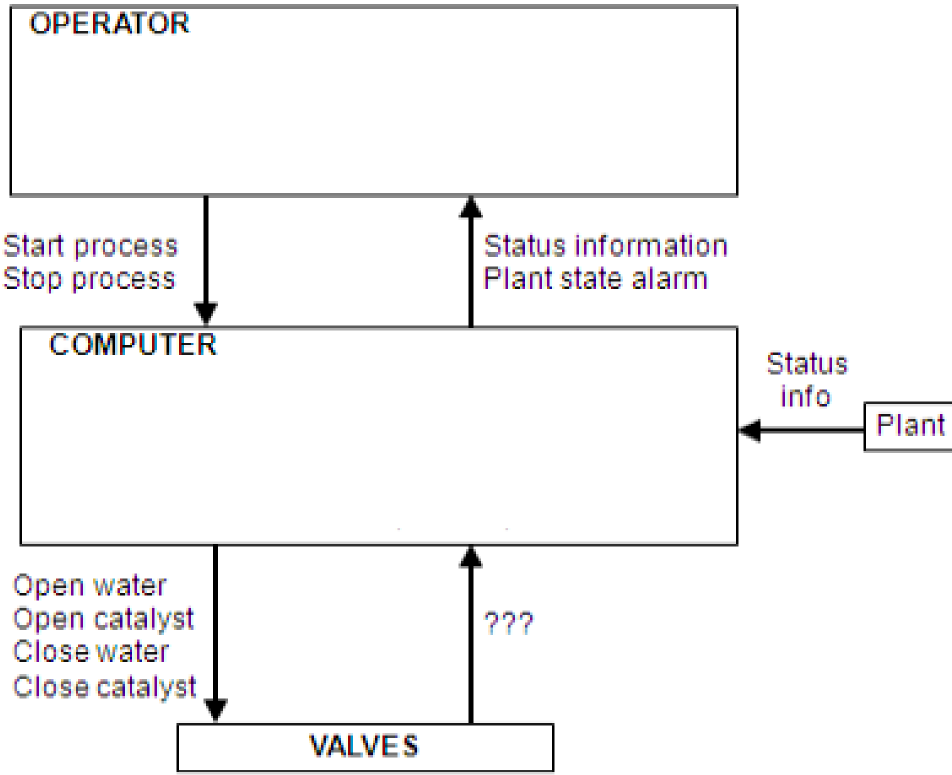
Control Structure:



	?	?	?	?
Close Water Valve				

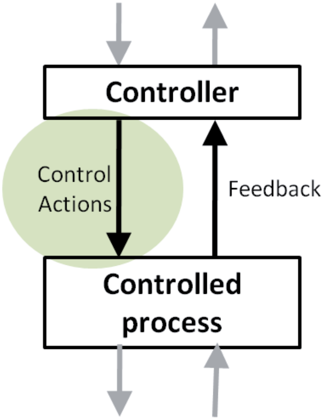
Chemical Reactor: Unsafe Control Actions

Control Structure:



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve	?	Computer closes water valve while catalyst open	?	?

Structure of an Unsafe Control Action



Example:

“Computer provides close water valve command when catalyst open”

Source Controller

Type

Control Action

Context

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller’s command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

Chemical Reactor:
Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve		Computer closes water valve while catalyst open	Computer closes water valve before catalyst closes	
Open Water Valve				
Open Catalyst Valve				
Close Catalyst Valve				

Chemical Reactor: Unsafe Control Actions (UCA)

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Water Valve		Computer closes water valve while catalyst open	Computer closes water valve before catalyst closes	
Open Water Valve	Computer does not open water valve when catalyst open		Computer opens water valve more than X seconds after open catalyst	Computer stops opening water valve before it is fully opened
Open Catalyst Valve		Computer opens catalyst valve when water valve not open	Computer opens catalyst more than X seconds before open water	
Close Catalyst Valve	Computer does not close catalyst when water closed		Computer closes catalyst more than X seconds after close water	Computer stops closing catalyst before it is fully closed

Safety Constraints

Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	?
Computer closes water valve while catalyst valve open	?
Computer closes water valve before catalyst valve closes	?
Computer opens catalyst valve when water valve not open	?
Etc.	Etc.

Safety Constraints

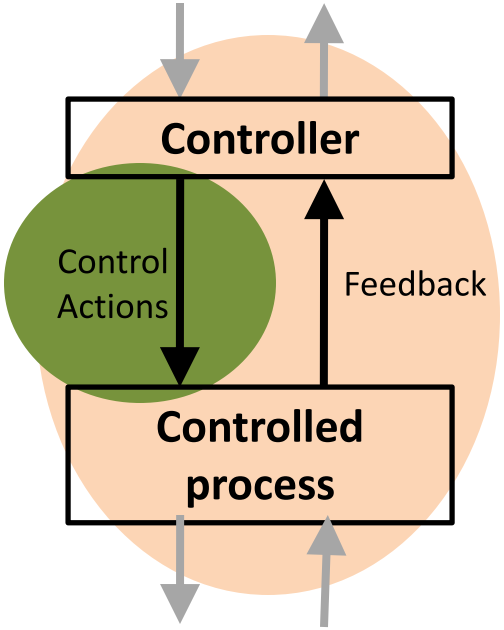
Unsafe Control Action	Safety Constraint
Computer does not open water valve when catalyst valve open	Computer must open water valve whenever catalyst valve is open
Computer opens water valve more than X seconds after catalyst valve open	Computer must open water valve within X seconds of catalyst valve open
Computer closes water valve while catalyst valve open	Computer must not close water valve while catalyst valve open
Computer closes water valve before catalyst valve closes	Computer must not close water valve before catalyst valve closes
Computer opens catalyst valve when water valve not open	Computer must not open catalyst valve when water valve not open
Etc.	Etc.

Traceability

- Always provide traceability information between UCAs and the hazards they cause.
  - Same for Safety Constraints and the hazards that result if violated.
- Two ways:
  - Create one UCA table (or safety constraint list) per hazard, label each table with the hazard
  - Create one UCA table for all hazards, include traceability info at the end of each UCA
    - E.g. **Computer closes water valve while catalyst open [H-1]**

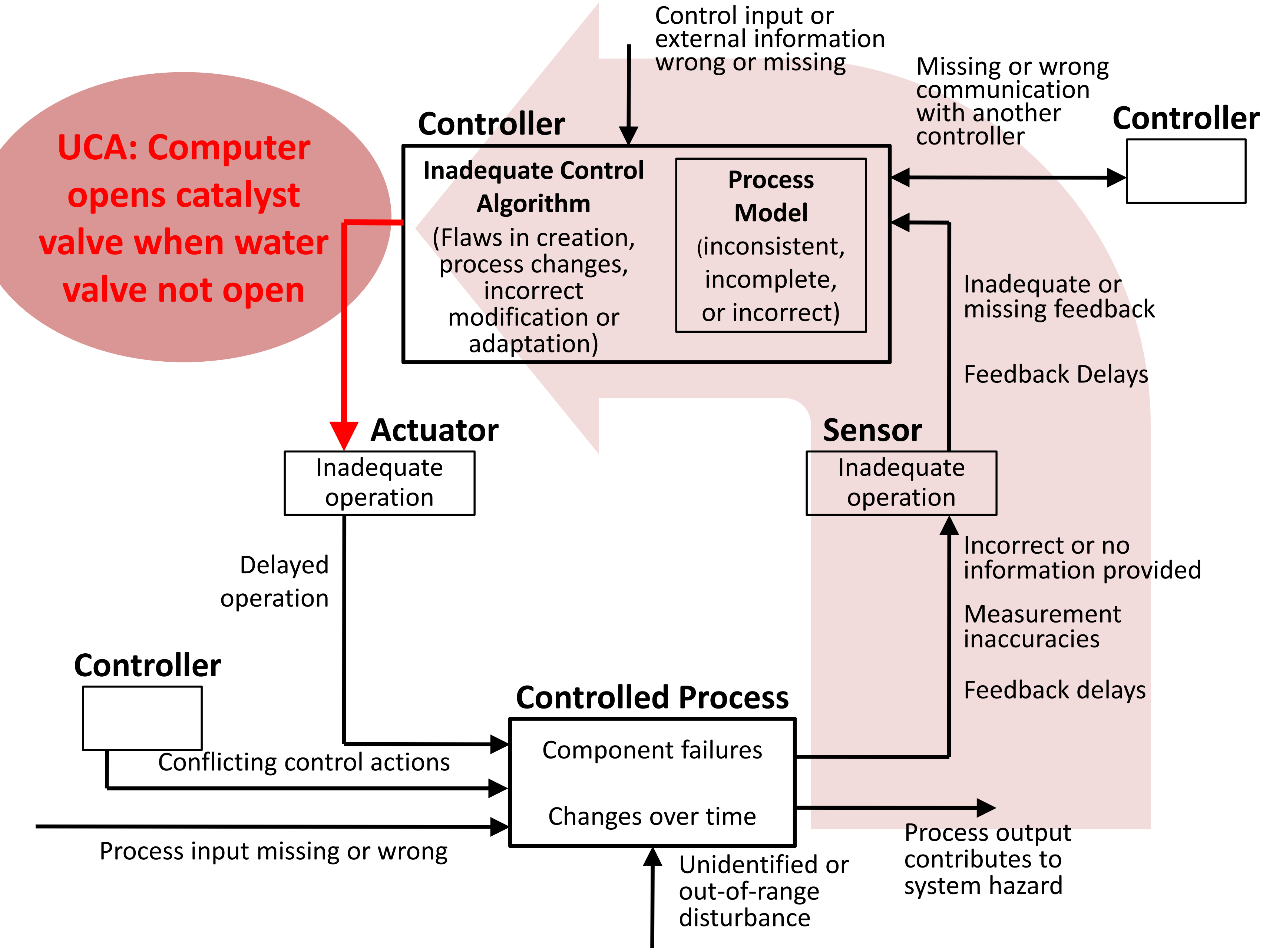
STPA
(System-Theoretic Process Analysis)

- ✓ Identify accidents and hazards
- ✓ Draw the control structure
- ✓ Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios



(Leveson, 2012)

Step 2: Potential causes of UCAs



UCA: Computer opens catalyst valve when water valve not open

Control input or external information wrong or missing

Controller

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Process Model (inconsistent, incomplete, or incorrect)

Missing or wrong communication with another controller

Controller

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate operation

Sensor

Inadequate operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Delayed operation

Controller

Conflicting control actions

Controlled Process

Component failures

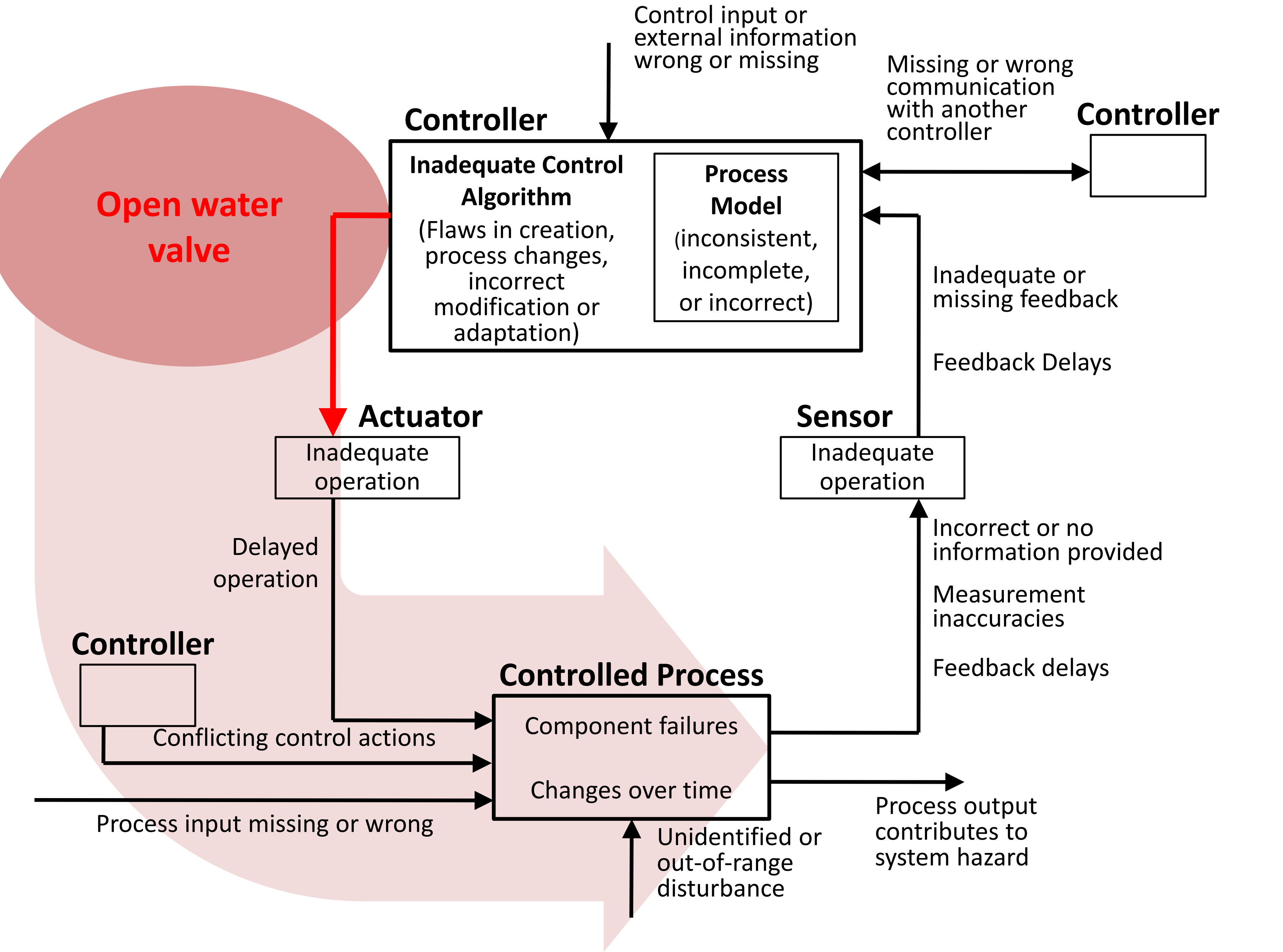
Changes over time

Process input missing or wrong

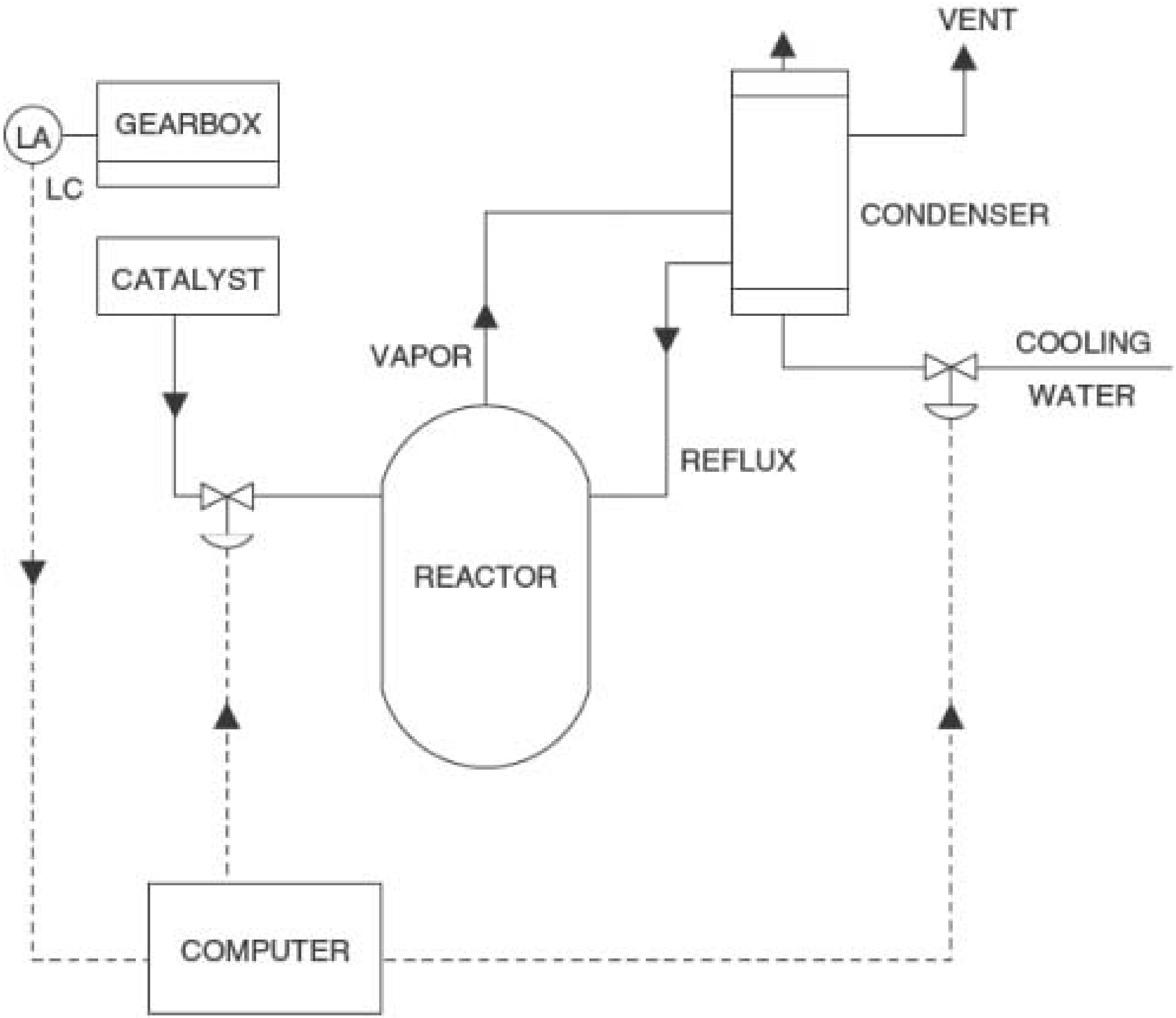
Unidentified or out-of-range disturbance

Process output contributes to system hazard

Step 2: Potential control actions not followed


Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Open water valve
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Chemical Reactor: Real accident


VENT
LA
GEARBOX
LC
CONDENSER
CATALYST
VAPOR
COOLING
WATER
REFLUX
REACTOR
COMPUTER